United States Government Accountability Office

GAO

Report to Congressional Committees

July 2011

INFORMATION TECHNOLOGY

DHS Needs to Improve Its Independent Acquisition Reviews

GAO-11-581

July 2011

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-11-581, a report to congressional committees

INFORMATION TECHNOLOGY

DHS Needs to Improve Its Independent Acquisition Reviews

Why GAO Did This Study

Since its creation in 2003, the Department of Homeland Security (DHS) has been developing new information technology (IT) systems to perform both mission-critical and support functions; however, it has faced challenges in developing these systems. One way to manage the inherent risks of developing and acquiring systems is through independent verification and validation (IV&V)—a process conducted by a party independent of the development effort that provides an objective assessment of a project's processes, products, and risks throughout its life cycle and helps ensure that program performance, schedule, and budget targets are met.

GAO was asked to determine (1) how DHS's IV&V policies and procedures for IT acquisitions compare with leading practices and (2) the extent to which DHS has implemented IV&V on its large IT system acquisitions. To do so, GAO assessed DHS's policy against industry standards and leading practice guides, as well as analyzed how eight selected IT programs had implemented IV&V.

What GAO Recommends

GAO recommends that DHS (1) update its acquisition policy to reflect elements of effective IV&V, (2) monitor and ensure implementation of this policy on applicable new and ongoing IT programs, and (3) collect data on IV&V usage and use it to evaluate the effectiveness of these investments. DHS concurred with GAO's recommendations and described actions planned or under way to address them.

View GAO-11-581 or key components. For more information, contact David A. Powner at (202) 512-9286 or pownerd@gao.gov.

What GAO Found

DHS recognizes the importance of IV&V and recommends its use on major IT programs. Nevertheless, its acquisition policy does not address the elements of leading practices for IV&V. Specifically, the department has not established risk-based decision making criteria for determining whether, or the extent to which, programs should utilize IV&V. In addition, department policy does not define the degree of independence required of agents and does not require that programs determine and document the planned scope of their efforts, including the program activities subject to review; the resources required; roles and responsibilities; and how the results will be reported and acted upon. Moreover, the policy does not address overseeing DHS's investment in IV&V. Thus, officials were unaware of the extent to which it was being used on major IT acquisition programs, associated expenditures, or if those expenditures are producing satisfactory results. Absent such policy elements and more effective oversight, the department's investments in IV&V efforts are unlikely to provide optimal value for the department and, in some cases, may even fail to deliver any significant benefits.

Many large IT acquisition programs across DHS reported using IV&V as part of their acquisition and/or development processes. Nevertheless, the eight major IT acquisition programs that GAO analyzed did not consistently implement the elements of leading practice. For example, the eight did not fully apply a structured, risk-based decision making process when deciding if, when, and how to utilize IV&V. (The table summarizes use of leading practices on the eight programs.) In part, these weaknesses are due to the lack of clear departmentwide guidance regarding the use of such practices. As a result, the department's IV&V efforts may not consistently contribute toward meeting IT acquisition cost, schedule, and mission goals.

Summary of DHS's Implementation of IV&V Leading Practices on Eight Large IT Acquisitions

IV&V leading practice	DHS program							
	A	B	C	D	E	F	G	H
Establish risk-based decision criteria	◐	◐	◐	◐	○	◐	○	○
Establish standards for independence	◐	◐	◐	◐	◐	◐	◐	◐
Define the scope of the effort	◐	◐	●	◐	○	◐	◐	◐
Determine the resources required	◐	◐	○	◐	○	○	◐	●
Establish program oversight	◐	◐	◐	◐	○	◐	◐	◐

Source: GAO analysis of DHS data, using code letters assigned by GAO.

Key: ● The program provided evidence that fully satisfied all elements.
◐ The program provided evidence that satisfied some, but not all elements.
○ The program provided evidence that did not satisfy any elements, or provided no evidence.

Contents

Figures

Abbreviations

ACE	Automated Commercial Environment
ARB	Acquisition Review Board
CBP	United States Customs and Border Protection
CFO	chief financial officer
CIO	chief information officer
CPO	chief procurement officer
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
DHS	Department of Homeland Security
ICE	Immigration and Customs Enforcement
IEEE	Institute of Electrical and Electronics Engineers
IT	information technology
ITIP	Information Technology Infrastructure Program
ITP	Infrastructure Transformation Program
NASA	National Aeronautics and Space Administration
NCPS	National Cybersecurity Protection Systems
NPPD	National Protection and Programs Directorate
IV&V	independent verification and validation
TASC	Transformation and System Consolidation
TECS-Mod	TECS-Modernization
Transformation	United States Citizenship and Immigration Services Transformation Program
TSA	Transportation Security Administration
USCG	United States Coast Guard
USCIS	United States Citizenship and Immigration Services
V&V	verification and validation

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

July 28, 2011

The Honorable Joseph I. Lieberman
Chairman
The Honorable Susan M. Collins
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Tom Carper
Chairman
The Honorable Scott P. Brown
Ranking Member
Subcommittee on Federal Financial Management,
Government Information, Federal Services and
International Security
Committee on Homeland Security and Governmental Affairs
United States Senate

The Department of Homeland Security (DHS) is charged with leading national efforts to secure America by deterring terrorist attacks, ensuring the nation's borders are safe and secure, and welcoming lawful immigrants and visitors, among other tasks. After it began operations in March 2003, DHS began developing information technology (IT) systems to perform both mission-critical and support functions. These systems included the acquisition of an integrated financial management system, the IT infrastructure to support the Secure Border Initiative Network (SBInet) "virtual fence" along the nation's southwest border, and the Coast Guard's (USCG) Rescue 21 system that supports its search and rescue operations off our nation's shores. DHS has faced challenges in developing these and other systems, which have resulted in schedule delays, cost increases, and not delivering the sought-after capabilities.[1]

Independent verification and validation (IV&V) is a process whereby organizations can reduce the risks inherent in system development and acquisition efforts by having a knowledgeable party who is independent of

[1]GAO, *Department of Homeland Security: Billions Invested in Major Programs Lack Appropriate Oversight,* GAO-09-29 (Washington, D.C.: Nov. 18, 2008).

the developer determine whether the system or product meets the users' needs and fulfills its intended purpose. We have previously recognized the use of IV&V as a leading practice for federal agencies in the acquisition of programs that are variously complex, large-scale, or high risk.[2] Congress has also previously required its implementation as one of several conditions for the obligation of funds for several high risk DHS IT acquisitions, including U.S. Customs and Border Protection's (CBP) SBInet and Automated Commercial Environment (ACE).[3]

As agreed, our objectives were to determine (1) how DHS's IV&V policies and procedures for IT acquisitions compare with leading practices and (2) the extent to which DHS has implemented IV&V on its large IT system acquisitions. To accomplish this, we researched the IV&V policies of recognized leading practices guides, industry standards, and other federal departments and agencies; analyzed relevant DHS department and component-level policies and guidance; and conducted interviews with relevant department and component-level officials. We then identified eight large IT system acquisitions from DHS components for further study using specific criteria. For these eight, we analyzed relevant program documentation, including IV&V plans, statements of work and reports from IV&V service providers, and DHS's Acquisition Review Board (ARB) decision memoranda.

We conducted this performance audit from March 2010 to July 2011, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. See appendix I for a complete description of our objectives, scope, and methodology.

[2]See GAO, *Homeland Security: Recommendations to Improve Management of Key Border Security Program Need to Be Implemented,* GAO-06-296 (Washington, D.C.: Feb. 14, 2006); *Homeland Security: U.S. Visitor and Immigrant Status Indicator Technology Program Planning and Execution Improvements Needed*, GAO-09-96 (Washington, D.C.: Dec. 12, 2008); and *Information Technology: Actions Needed to Fully Establish Program Management Capability for VA's Financial and Logistics Initiative,* GAO-10-40 (Washington, D.C.: Oct. 26, 2009).

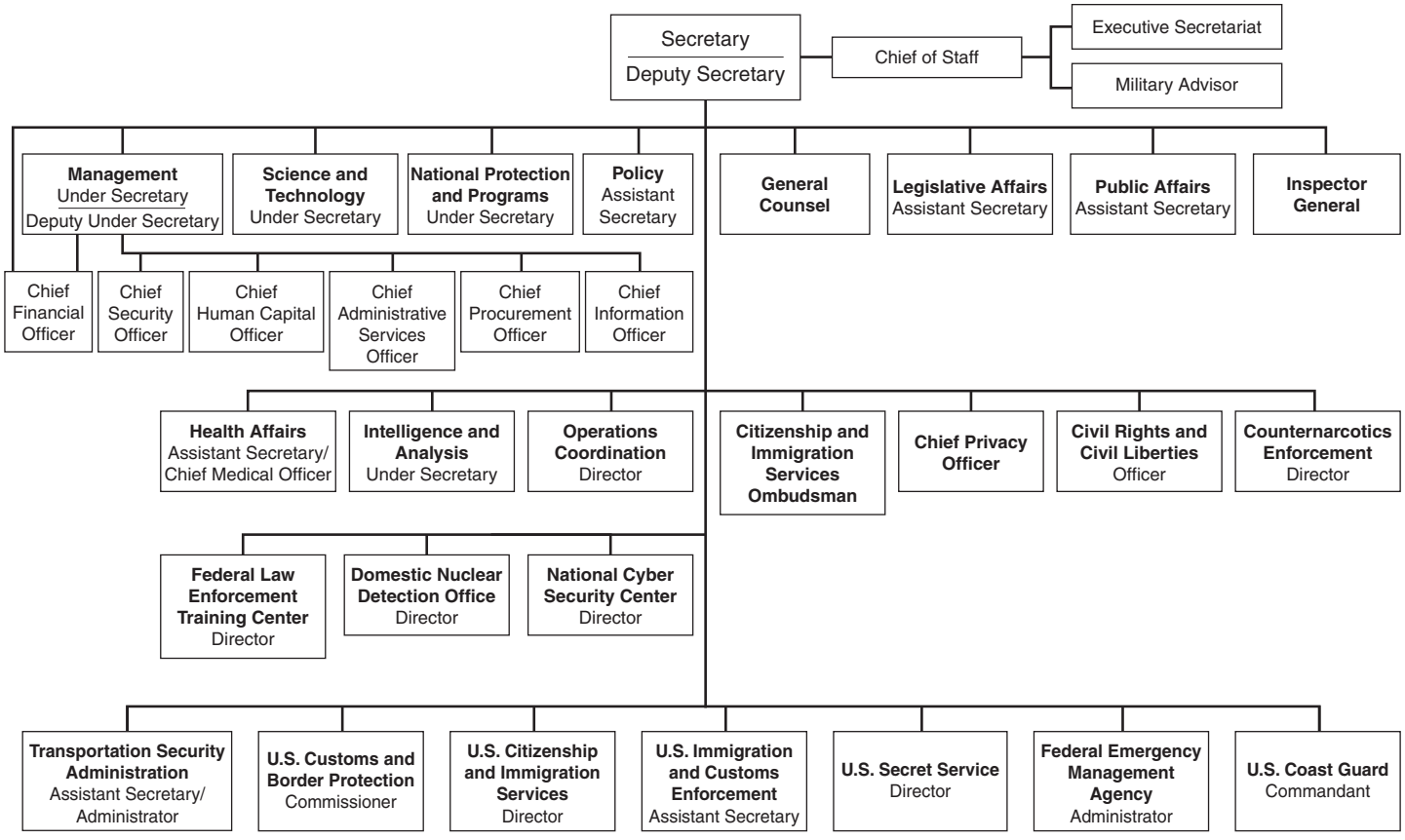
[3]Pub. L. No. 109-295, 120 Stat. 1355, 1359-60 (Oct. 4, 2006).

Background

DHS's mission is to lead the unified national effort to secure America by preventing and deterring terrorist attacks and protecting against and responding to threats and hazards to the nation. DHS is also responsible for ensuring that the nation's borders are safe and secure, welcoming lawful immigrants and visitors, and promoting the free flow of commerce.

Created in 2003, DHS assumed control of about 209,000 civilian and military positions from 22 agencies and offices that specialize in one or more aspects of homeland security. The intent behind the merger that created DHS was to improve coordination, communication, and information sharing among these multiple federal agencies. Figure 1 shows DHS's organizational structure; table 1 identifies DHS's principal organizations and describes their missions.

Figure 1: DHS Organizational Structure



Source: GAO depiction of DHS information.

Table 1: DHS's Principal Component Organizations and their Missions

Principal organizations[a]	Mission
U.S. Customs and Border Protection (CBP)	Protects the nation's borders to prevent terrorists and terrorist weapons from entering the United States, while facilitating the flow of legitimate trade and travel.
Domestic Nuclear Detection Office	Protects the nation by detecting and reporting unauthorized attempts to import, possess, store, develop, or transport nuclear or radiological material for use against the nation.
Federal Emergency Management Agency	Prepares the nation for hazards, manages federal response and recovery efforts following any national incident, and administers the National Flood Insurance Program.
U.S. Immigration and Customs Enforcement (ICE)	Protects the nation's borders by identifying and limiting vulnerabilities in the nation's border, economic, transportation, and infrastructure security.
Intelligence and Analysis	Works closely with DHS components, as well as state, local, and tribal entities, to fuse nontraditional and traditional intelligence information streams into national threat assessments, and disseminates the resulting information to DHS and external homeland security customers.
Management Directorate	Oversees department budgets and appropriations, expenditure of funds, accounting and finance, procurement, human resources, IT, facilities and equipment, and identifies and tracks performance measurements. Includes the Offices of the Chief Information Officer (CIO), Chief Financial Officer (CFO), and Chief Procurement Officer (CPO).
National Protection and Programs Directorate (NPPD)	Works with state, local, and private sector partners to identify threats, determine vulnerabilities, and target resources where risk is greatest to safeguard the nation's critical physical and cyber infrastructures.
Office of Health Affairs	Protects the nation against biohazards through coordinated efforts with all levels of government and the private sector to develop and support a scientifically rigorous, intelligence-based biodefense and health preparedness architecture.
Office of Operations and Coordination Planning	Monitors the security of the United States and coordinates activities within the department and with governors, homeland security advisors, law enforcement partners, and critical infrastructure operators in all 50 states and in more than 50 major urban areas nationwide.
Transportation Security Administration (TSA)	Protects the nation's transportation systems to ensure freedom of movement for people and commerce.
U.S. Citizenship and Immigration Services (USCIS)	Administers immigration and naturalization adjudication functions and establishes immigration services policies and priorities.
U.S. Coast Guard (USCG)	Protects the public, the environment, and U.S. economic interests in the nation's ports and waterways, along the coast, in international waters, and in any maritime region as required to support national security.
U.S. Secret Service	Protects the President and other high-level officials and investigates counterfeiting and other financial crimes, including financial institution fraud; identity theft; computer fraud; and computer-based attacks on our nation's financial, banking, and telecommunications infrastructure.

Source: GAO analysis of DHS data.

[a]This table does not show the organizations that fall under each of the directorates. This table also does not show all organizations that report directly to the DHS Secretary and Deputy Secretary, such as executive secretary, legislative and intergovernmental affairs, public affairs, chief of staff, inspector general, and general counsel.

Not since the creation of the Department of Defense in 1947 has the federal government undertaken a transformation of this magnitude. As we reported before the department was created, such a transformation is critically important and poses significant management and leadership challenges. For these reasons, we designated the implementation of the department and its transformation as high risk in 2003,[4] and we continue to do so today.[5] In this regard, we have stated that failure to effectively address DHS's management challenges and program risks could have serious consequences for our national security.[6]

DHS IT Acquisitions and Their Management

In support of its organizational transformation and in response to the nation's evolving security needs, DHS has been spending billions of dollars each year to develop and acquire IT systems to perform both mission-critical and support functions, which frequently must be coordinated among components, as well as among external entities. For fiscal year 2010, DHS expected to spend approximately $6.3 billion on 348 IT-related programs, which included 53 major IT acquisition programs that were designated for oversight by the DHS Under Secretary for Management.[7] We refer to these 53 programs as "large acquisitions" throughout this report. Table 2 describes the programs relevant to this review.

[4]GAO, *High-Risk Series: An Update*, GAO-03-119 (Washington, D.C.: January 2003).

[5]GAO, *High-Risk Series: An Update*, GAO-11-278 (Washington, D.C.: February 2011).

[6]GAO, *Homeland Security: Despite Progress, DHS Continues to Be Challenged in Managing Its Multi-Billion Dollar Annual Investment in Large-Scale Information Technology Systems,* GAO-09-1002T (Washington, D.C.: Sept. 15, 2009).

[7]A DHS major system is one where the total life cycle costs for the system are estimated to equal or exceed $300 million. DHS identified a total of 348 IT-related programs for fiscal year 2010. This review focuses on a subset of those—the 53 IT programs on the DHS Major Acquisition Oversight List established by the Under Secretary for Management on May 26, 2010 (which also contained non-IT acquisition programs). During our review, 12 programs were defunded, recategorized to level 3 or non-IT, or taken off the Major Acquisition Oversight List, and therefore are not discussed in this report.

Table 2: Examples of Major DHS IT Acquisition Programs

DHS component and acquisition program	Description
CBP—Automated Commercial Environment (ACE)/International Trade Data System[a]	Initiated in 2001 to support Title VI of the North American Free Trade Agreement Implementation Act (commonly known as the Customs Modernization Act), this program is to incrementally replace existing cargo processing technology systems with a single system for land, air, rail, and sea cargo and serve as the central data collection system for federal agencies needing access to international trade data in a secure, paper-free, Web-enabled environment.
ICE—TECS-Modernization (TECS-Mod)	This program is to replace the legacy mainframe system developed by the U.S. Customs Service in the 1980s to support its inspections and investigations. Following the creation of DHS, those activities were assigned to CBP and ICE, respectively. CBP and ICE are now working to modernize their respective portions of the system in a coordinated effort with separate funding and schedules. ICE's portion of the program will include modernizing the investigative case management and related support modules of the legacy system.
NPPD—National Cybersecurity Protection Systems (NCPS)[a]	This program is to reduce the federal government's vulnerability to cyber threats by decreasing the frequency of cyberspace disruptions and minimizing the duration and damage of those disruptions. It is expected to provide capabilities in four cyber mission areas: (1) threat alter, warning, and analysis; (2) coordination and collaboration; (3) response and assistance; and (4) protection and detection.
Office of the CFO—Transformation and System Consolidation (TASC)	Initiated in 2007, this program is to modernize, transform, and integrate the various financial acquisition and asset management systems in use at the department's components. It plans to adopt a commercial off-the-shelf package that is already configured and in use in the public sector. In May 2011, a DHS official stated that TASC is to be cancelled.
Office of the CIO—Infrastructure Transformation Program (ITP)	This program is to contribute to DHS's consolidated infrastructure investment, supporting areas such as data center, network, e-mail consolidation, and single sign on. It is also expected to lead to efficiencies across DHS's IT environment.
TSA—Information Technology Infrastructure Program (ITIP)	This program is intended to provide comprehensive technical infrastructure support for TSA in four main program areas: (1) office automation, (2) infrastructure, (3) program management, and (4) contract support. It is intended to address IT equipment and service needs across various government and industry contracts that will technically support and expand the IT capabilities of the agency's international workforce.
USCG—Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR)[a]	This program is to provide an interoperable network that combines information from USCG assets and sensors to allow commanders to collect and fuse relevant information and direct and monitor assigned forces and first responders across the range of operations.
USCIS—Transformation Program (Transformation)	A 5-year effort to modernize component-wide business processes and technology, Transformation is to move USCIS from a paper-based filing system to a centralized, consolidated, electronic adjudication filing system.

Source: DHS.

[a]This program was previously assessed in GAO, *Department of Homeland Security: Assessments of Selected Complex Acquisitions*, GAO-10-588SP (Washington, D.C.: June 30, 2010).

In order to manage these acquisitions, the department finalized an acquisition life cycle and review process in 2010, and established the Management Directorate, headed by the Under Secretary for Management, which houses both the Chief Information Officer (CIO) and Chief Procurement Officer (CPO).[8] The CIO's responsibilities include setting departmental IT policies, processes, and standards, and ensuring that IT acquisitions comply with DHS IT management processes, technical requirements, and approved enterprise architecture, among other things. Additionally, the CIO chairs DHS's Chief Information Officer Council, which is responsible for ensuring the development of IT resource management policies, processes, best practices, performance measures, and decision criteria for managing the delivery of IT services and investments, while controlling costs and mitigating risks. The CPO is the department's senior procurement executive, who has leadership and authority over DHS acquisition and contracting, including major investments. The CPO office's responsibilities include issuing acquisition policies and implementation instructions, overseeing acquisition and contracting functions, and ensuring that a given acquisition's contracting strategy and plans align with the intent of the department's ARB, the department's highest investment review board.

DHS's acquisition management directive defines four acquisition life cycle phases that are to ensure consistent and efficient management, support, review, and approval for programs across the department. Each phase culminates in an ARB review on whether a program is ready to proceed to the next life cycle phase. The ARB's chairperson is responsible for determining the readiness of a program and for approving the key acquisition documents critical to establishing a program's business case, operational requirements, acquisition baseline, and testing and support plans. Also, the ARB's chairperson is responsible for assessing breaches of the acquisition plan's cost and schedule baselines and directing corrective actions.

Other DHS entities share responsibility for IT management and procurement activities. For example, control of IT management functions is shared by the DHS CIO and CIOs at the major organizational components (e.g., directorates, offices, and agencies). Similarly, DHS

[8]Department of Homeland Security, *Acquisition Management Directive, Directive Number 102-01* (Jan. 20, 2010).

relies on a structure of dual accountability and collaboration between the CPO and the heads of DHS components to carry out the acquisition function. DHS components have also designated component acquisition executives to serve as the senior acquisition officials within the components and to be responsible for implementation of management and oversight of all component acquisition processes.

GAO Has Previously Reported That DHS Is Not Effectively Managing and Overseeing Its Major IT Acquisitions

Since its creation, DHS has faced challenges in acquiring large IT systems, leading to cost and schedule overruns on multiple programs. Our November 2008 report[9] on DHS's oversight of major acquisition programs described several of these challenges. Specifically,

- DHS had not effectively implemented or adhered to its investment review process;
- DHS had not consistently enforced decisions that were reached by the investment review board because the department did not track whether components and offices had taken the actions required by the board; and
- two of nine components did not have the required component-level review processes to adequately manage their major investments.

Accordingly, we made a series of recommendations to DHS to address weaknesses in departmentwide acquisition policies and practices and with individual programs, such as reinstating the department's oversight board to review and approve acquisition requirements and assess potential duplication of effort, and directing that component heads establish a mechanism to ensure that major investments comply with established component and departmental investment review policy standards. The department generally concurred with our findings and recommendations, citing actions that had been taken and efforts under way to improve the investment review process.

In September 2009 and again in June of 2010,[10] we reported on the status of DHS's acquisition improvement efforts and on selected major

[9]GAO-09-29.

[10]GAO-09-1002T and GAO-10-588SP.

acquisition programs. Despite some progress, we found that many of DHS's major system acquisitions were still not receiving effective oversight and that DHS continued to face challenges in fully defining and implementing key system investment and acquisition management policies and procedures. Among other things, we noted that

- the ARB had begun to meet more frequently than in the past and had reviewed dozens of major acquisition programs, but more than 40 programs had not been reviewed, and programs did not consistently implement review action items by established deadlines;
- nearly 80 percent of major programs lacked basic acquisition documents, and a database established to track key program information—such as cost and schedule performance and program risks—relied on self-reported program data rather than independently verified data; and
- component acquisition review processes were not fully in place, and components' efforts to implement department oversight directives and sufficiently staff the associated processes were not yet complete.

We concluded that, while the department had made progress in establishing key institutional acquisition and IT investment management-related controls and implementing them on large-scale programs, considerable effort remained before the department could be considered a mature IT system acquirer and investor and that our prior recommendations continued to provide the department with a framework to guide its efforts.

IV&V Can Reduce Risk in Developing and Acquiring Large-Scale IT Systems

IV&V is a process whereby organizations can reduce the risks inherent in system development and acquisition efforts by having a knowledgeable party who is independent of the developer determine that the system or product meets the users' needs and fulfills its intended purpose. IV&V involves proactively determining early in a program's life cycle what its risks are likely to be, and then identifying those that could be mitigated or lessened by performing additional reviews and quality assessments. IV&V activities can help ensure that quality is built into program deliverables from the beginning—starting with business and requirements analysis, continuing through software development and unit-testing activities, and ending with system and integration testing and acceptance.

We have previously identified IV&V as a leading practice for large and complex system development and acquisition programs.[11] In addition, a review published in 1999 by the Institute of Electrical and Electronics Engineers (IEEE)[12] found that IV&V had a measurable beneficial effect on a program's development. For example, it

- promoted the earlier detection of system faults,
- identified a greater number of faults,
- helped to reduce the average time it takes to fix faults, and
- enhanced operational correctness.

The study concluded that any process that systematically applies well-designed IV&V activities to a structured software development process would result in similar benefits.

Typically, IV&V is performed by an agent that is independent of the development organization to obtain unbiased reviews of a system's processes, products, and results, with the goal of verifying and validating that these meet stated requirements, standards, and user needs. As such, we have reported[13] that IV&V is work above and beyond the normal quality assurance and performance review activities performed during system development and acquisition. This work must not substitute for the developer's responsibility, but should complement and reinforce the developer's system engineering processes, configuration management, and qualification test functions. According to recognized industry standards,[14] IV&V can provide management with an objective assessment of a program's processes, products, and risks throughout its life cycle and help ensure conformance to program performance, schedule, and budget targets. Furthermore, it can help facilitate the early

[11]See GAO-09-96 and GAO-10-40.

[12]See Institute of Electrical and Electronics Engineers, Inc., "Evaluating the Effectiveness of Independent Verification and Validation," (October 1999: 79-83).

[13]GAO, *Space Station: NASA's Software Development Approach Increases Safety and Cost Risks,* GAO/IMTEC-92-39 (Washington, D.C.: June 19, 1992).

[14]Institute of Electrical and Electronics Engineers, Inc., *IEEE Standard for Software Verification and Validation*, IEEE Std 1012-2004 (New York, N.Y.: June 8, 2005).

detection and correction of system anomalies and support the system's conformance to performance, schedule, and budget goals, among other benefits.

We have previously identified the independence of the responsible agent as a key aspect of IV&V's value to the IT acquisitions process.[15] Independence is defined by the following three components:

- *Technical independence*–requires the effort to be performed by personnel who are not involved in the development of the system. This ensures that the IV&V team brings a fresh viewpoint to the analysis of the system development process and its products.

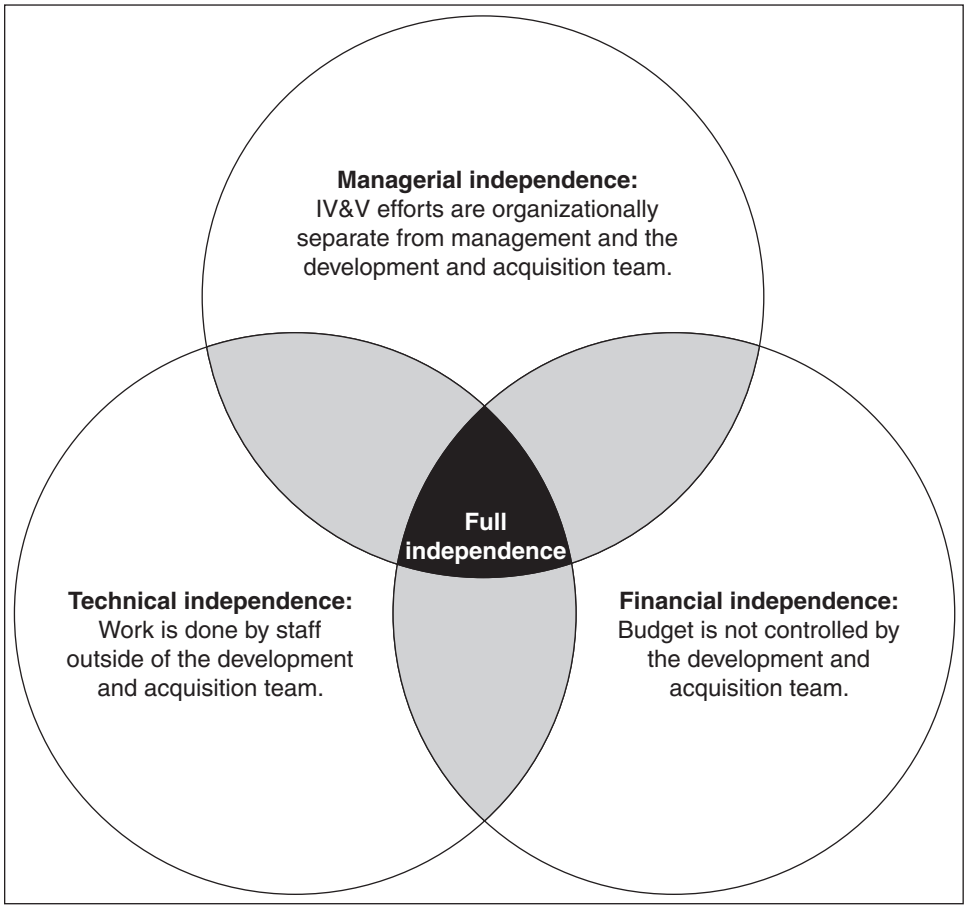
- *Managerial independence*–requires that the agent be managed separately from the development and program management organizations. The effort must be allowed to freely select the system components or segments it will analyze and test, and the test and analysis techniques it will use. The agent must also be allowed to freely report its findings to program management, without prior approval from the development group.

- *Financial independence*–requires that the funding for IV&V be controlled by an organization separate from the development organization. This ensures that the effort will not be curtailed by having its funding diverted to other program needs, and that financial pressures cannot be used to influence the effort.

An IV&V effort that exhibits all three of these characteristics is fully independent (see fig. 2). Rigorous independence from the development or acquisition effort ensures that IV&V's insights into a program's processes and associated work products are objective.

[15]See GAO-06-296 or *Financial Management Systems: DHS Faces Challenges to Successfully Consolidating Its Existing Disparate Systems,* GAO-10-76 (Washington, D.C.: Dec. 4, 2009).

Figure 2: Components of IV&V Independence



Source: GAO analysis of recognized practices.

Verification and validation (V&V) are related processes intended to provide evidence that developed or acquired products meet specified requirements and that they fulfill their intended use when placed in their intended environment, respectively. V&V practitioners gather this information through the assessment, analysis, evaluation, review, inspection, and testing of system engineering products and processes. In other words, verification ensures that "you built the product right," while validation ensures that "you built the right product."

Table 3 illustrates IV&V activities and work products for a typical development/acquisition life cycle.

Table 3: Illustrative IV&V Activities and Work Products by Life Cycle Phase

System life cycle phases	IV&V activities	Work products
Planning	• Provide an independent estimate of likely program costs	• Independent cost assessment
Requirements analysis	• Assess the validity and analyze the quality of documented program requirements	• Requirements evaluation reports (such as system requirements review, traceability, and interface analyses)
Design	• Ensure that proposed design is aligned with stated program requirements and mission needs	• Concept and design evaluation reports (such as concept documentation evaluation and contract verification reports)
Integration	• Review security-related risks and/or vulnerabilities inherent in the system design • Assess system for any likely issues with component inter-operability	• Security analysis reports • Integration test plan • Anomaly reports • Configuration management assessments
Testing	• Review and assess system test plans for appropriate scope and methods • Evaluate test results	• Test evaluation reports • Operational readiness evaluation reports

Source: Summary of GAO analysis of industry leading practices.

IV&V activities may also focus on program management activities and work products across the development/acquisition life cycle. For example, the agent may be involved in the program's risk management efforts by identifying new risks, or by providing recommendations to eliminate, reduce, or mitigate risks. The agent may also provide an independent view of the program's progress in terms of its ability to meet cost, schedule, or performance commitments.

Congress has recognized the value of IV&V, in that it has previously required its implementation as one of several conditions for the obligation of funds for certain acquisitions at DHS. For example, Congress directed the department to certify that an IV&V agent was under contract as a

condition for obligating funds in fiscal year 2007 for ACE, SBInet, and the U.S. Visitor and Immigrant Status Indicator Technology program.[16] In addition, the Deputy Administrator of E-Government and Information Technology at the Office of Management and Budget told us that he has seen the value of the practice during their reviews of major investments, although its use is not required at federal agencies.

Our review[17] of leading practices from industry and across the federal government[18] identified several key elements of effective IV&V, which are described here along with examples we obtained from examining the policies of several federal departments and agencies contacted during this review.

- *Decision criteria.* When deciding to perform IV&V, risk-based criteria should be used to determine which programs, or aspects of programs, should be subject to review. In other words, the determination to conduct IV&V and its extent should be made on the basis of the relative mission criticality of the program and its components, as well as on the potential impacts to the program from undetected system errors, immaturity of the technology to be used, and unreliability of program schedule and cost estimates, among other program risks. For example, NASA policy states that the IV&V Board of Advisors provides recommendations to the Chief, Safety and Mission Assurance, for implementing IV&V on specific programs, based on specific criteria such as technical complexity, human safety, consequences of failure, program costs, and required time frames. The chief then authorizes IV&V for the programs with the highest risk profiles.

- *Standards for independence.* Organizations should also include standards that describe the degree of technical, managerial, and financial independence required of the personnel or agents

[16]Pub. L. No. 109-295, 120 Stat. 1355, 1357-60 (Oct. 4, 2006).

[17]Our analysis identified five primary sources of IV&V guidance; see appendix I for the sources and further details of our methodology.

[18]We contacted 10 federal departments and administrations concerning their IV&V policies. These 10 departments had the largest average IT spending per major investment for fiscal years 2008 through 2010. They were: the Department of Defense, Department of Veterans Affairs, National Aeronautics and Space Administration, Department of Justice, Social Security Administration, Department of State, Department of Energy, DHS, Department of Transportation, and Department of Commerce.

performing IV&V. Having standards for independence helps to ensure that the results of activities are reported to program oversight officials, as well as to program management. In this regard, NASA has established an agencywide program for managing all of the system software IV&V efforts. The program includes an internal organization that functions as their IV&V agent and that has no technical, managerial, or financial ties to the development organization.[19]

- *Defined scope of the effort.* The effort should document which program development or acquisition activities will be subject to IV&V. Examples of such activities may include: requirements evaluation, concept/design evaluation, risk evaluation, risk management procedures evaluation, configuration management procedures evaluation, test evaluation, operational readiness evaluation, and cost estimate evaluation. Further, compliance criteria should be established for each activity. For example, NASA's IV&V technical framework has defined assessment procedures for various system development activities, along with related pass/fail criteria.

- *Required program resources.* Plans should identify the required personnel, funding, facilities, tools, and methods that will be required to perform the activities necessary for the defined scope of the IV&V effort. For example, the Federal Bureau of Investigation requires identification of staff, tools, and training necessary to perform IV&V activities and to develop and maintain work products.

- *Management and oversight.* As with any investment, organizations should conduct proper management and oversight of their IV&V efforts. For example, in order to effectively manage the effort, the roles and responsibilities of all parties involved should be specified and a process for responding to issues raised by the effort should be defined. Several agencies we spoke with had established policies that defined the roles and responsibilities of parties involved in their IV&V process. For example, the Federal Bureau of Investigation's policy defines the relationship between the program manager, the developer/integrator, and the contractor, including distribution channels for program artifacts, assessments, and deliverables.

[19]In 1993, NASA adopted an agencywide strategy to provide assurance that safety and mission critical software would operate correctly, safely, and dependably. Because software failures have meant lost investments, mission failures, and risk to life, NASA developed an IV&V policy to mitigate these risks.

Further, organizations should also provide the means for senior management to obtain timely information regarding the progress of their IV&V investments in terms of cost, capability, timeliness, and quality.

Concerning IV&V oversight, organizations should evaluate the effectiveness of their efforts. A variety of guidance[20] recommends that organizations should actively monitor service providers to ensure that they are effective in delivering services and meeting requirements. Moreover, organizations should ensure that sufficient information about their IV&V investments is maintained to support current and future investment decisions and to highlight lessons learned. For example, NASA has found over the years that the application of rigorous IV&V has provided a positive return on investment, and has taken steps to assess the quality and consistency of their efforts through its Technical Quality and Excellence group, which examines IV&V results across all projects and ensures that efforts were conducted in accordance with approved guidelines and standards.

DHS's IT Acquisition Policy Does Not Incorporate Key Elements of Effective IV&V

Adoption of IV&V can provide agencies with information to better manage their IT investments. To be effective, leading industry practices and government guidance recommend, among other things, that organizations adopt certain key elements of effective IV&V.

DHS's Acquisition Guidebook recognizes IV&V as a leading practice, recommends (though generally does not require) its use,[21] and cites the IEEE standard for V&V as the basis for IV&V. However, DHS's policy contains key gaps or ambiguities relative to each of the key elements of effective IV&V.

[20]See the IT Governance Institute's Control Objectives for Information and Related Technology (COBIT®) 4.1, the Software Engineering Institute's Capability Maturity Model Integration for Acquisition version 1.2, and GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity,* GAO-04-394G (Washington, D.C.: March 2004).

[21]While DHS's acquisition policy does not normally require large-scale IT acquisition programs to use IV&V, DHS policy does require its use in two cases: (1) if Congress mandates its use by a particular acquisition program or (2) if the DHS ARB requires that a program do so.

- *Decision criteria.* DHS policy does not specify a risk-based approach, does not define related criteria for making decisions regarding IV&V, and does not require component agencies to do so. Specifically, the department does not establish risk-based decision making criteria in its Acquisition Guidebook for determining whether, or the extent to which, IT programs should use it and does not require that programs conduct assessments against such criteria.

- *Standards for independence.* DHS acquisition policy does not address the independence of agents. DHS's policy does not define the required degree of independence that agents must demonstrate and does not require that its component agencies define such standards for themselves. Consequently, the policy does not specify mechanisms to ensure that efforts on major IT acquisitions are adequately objective. Moreover, the policy does not establish reporting mechanisms to ensure that the results of activities are reported to program oversight officials for use in DHS's investment management process.

- *Defined scope of the effort.* DHS does not require that the specific scope of efforts be defined. While department policy suggests performing IV&V on life cycle activities such as requirements definition, requirements management, and operational readiness activities, department policy does not require that its component agencies or acquisition programs critically assess their IT acquisition programs to determine and document the appropriate scope of IV&V efforts for each program. In addition, the policy does not require that such efforts identify and document compliance criteria for the validation and verification activities.

- *Required program resources.* DHS acquisition policy does not require (or require that its component agencies ensure) that IT acquisitions identify and document the resources needed to execute their efforts—including facilities and tools. It is also silent on other essential aspects of planning the effort, including funding and human resources.

- *Management and oversight.* DHS policy does not address IV&V management or the need to effectively oversee the department's investment in this practice. While DHS policy assigns certain responsibilities for agents and government officials, it does not require a process for responding to issues raised by the effort and does not require that its component agencies or their acquisition programs do so. In addition, officials at both the Office of the CIO and Office of the CPO stated that DHS does not track which programs across the

department employ IV&V unless a program is under a congressional mandate to do so. Further, DHS officials stated that they do not measure the effectiveness of IV&V efforts across the department. Thus, department officials were unaware whether or the extent to which IV&V was being used by the largest IT acquisition programs. They were also unaware of the department's total expenditures for IV&V, or if those expenditures (which total approximately $91 million across the eight programs we reviewed in detail) are producing satisfactory results.

Officials from the Office of the Chief Information Officer said that they attempted to address IV&V in their 2010 acquisition policy, but they agreed that the policy still contains gaps relative to how it is currently planned, executed, and overseen across the department. They stated that this was due to limited resources and other priorities. Further, they acknowledged that these gaps should be addressed and that the current policy was being revised.

Until DHS provides a clear departmentwide policy requiring programs to employ the key elements of effective IV&V, it is less likely to achieve the full potential of such efforts on its large acquisitions. Consequently, IV&V may not provide the intended benefits of ensuring that DHS's IT systems and their components meet quality standards, satisfy user needs, and operate as intended. Furthermore, in the absence of a clearly articulated risk-based decision framework for undertaking IV&V, applying its results, and evaluating its effectiveness, DHS's investments in IV&V efforts are unlikely to provide optimal value for the department and, in some cases, may even fail to deliver any significant benefits.

DHS Reports Widespread Use of IV&V, but Implementation of Key Elements Is Limited

Many large IT acquisitions from across DHS report using IV&V as part of their acquisition and/or development process. However, despite reports of this widespread use, we found that the department did not consistently implement key elements of IV&V on eight major IT acquisition programs. For example, none of the eight used a structured, risk-based decision making process when deciding if, when, and how to use IV&V. In part, these weaknesses can be attributed to the lack of clear departmentwide policy requiring the application of such elements. As a result, DHS's inconsistent use of IV&V may not reliably and significantly contribute toward meeting the schedule and mission goals of the department's major IT programs.

DHS Reports Widespread Use of IV&V on Large IT Programs

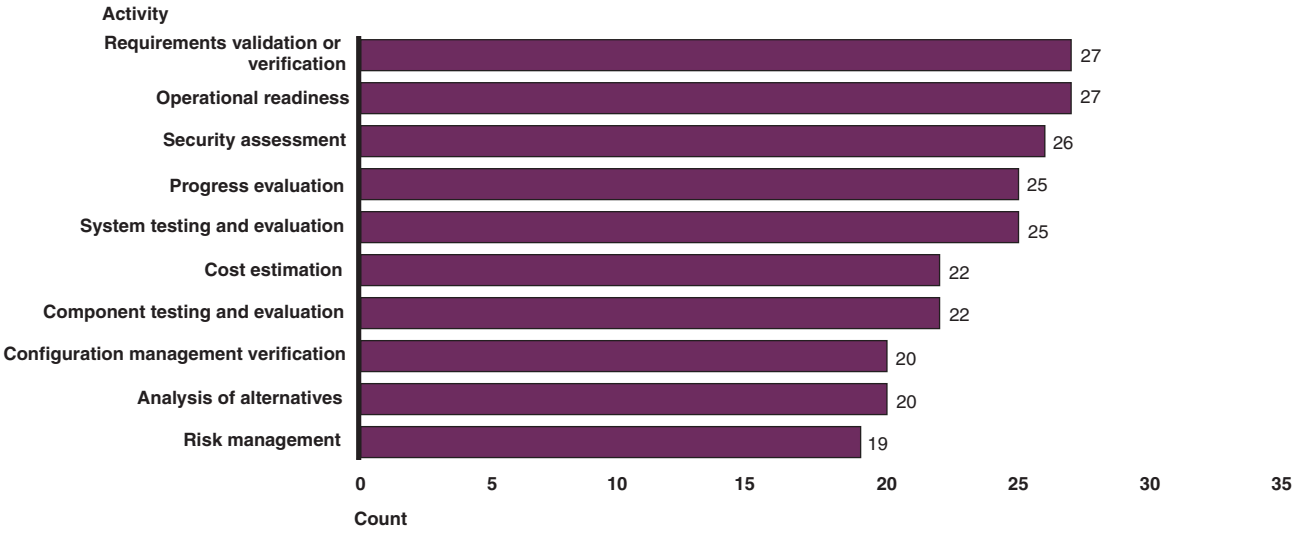
DHS's large IT programs reported widespread use of IV&V as part of their acquisition and/or development processes. Specifically, 35 of 41 major IT acquisition programs from DHS's oversight list reported that IV&V efforts were planned, under way, or completed. The specific IV&V activities reported for each program are listed in appendix II, along with other descriptive program information.[22]

The 35 programs reported using IV&V across a range of program activities.[23] For example, 26 of the programs reported performing IV&V on at least half of the life cycle activities listed in our questionnaire. Requirements validation and verification and operational readiness were the most commonly reported activities (reported by 27 of the 35 programs responding); risk management was the least reported activity (reported by 19 programs). (See fig. 3 for total responses on the activities we specifically identified in our questionnaire.) A few programs reported other IV&V activities, such as assessment of standards compliance; readiness of integrated logistics support; assessment of equipment usability; contract auditing; and compliance with the system engineering life cycle.

[22]DHS's Major Acquisition Oversight List, issued by the Under Secretary for Management on May 26, 2010, consists of 53 IT programs and other non-IT programs designated as level 1 or level 2 by the department. During our review, DHS reported that 12 programs were defunded, recategorized to level 3 or to non-IT, or taken off the oversight list; therefore, we did not include them in this report. Our review focused on the 41 remaining programs.

[23]The life cycle activities we collected data on were (1) independent cost estimation or cost estimate validation, (2) program progress and/or performance verification or evaluation, (3) requirements validation or verification, (4) design validation or alternatives analysis, (5) risk evaluation and management, (6) security vulnerability or security risk assessments, (7) configuration management verification, (8) component verification testing and evaluation, (9) system or integration verification testing and evaluation, (10) operational readiness testing and evaluation, and (11) other activities.

Figure 3: Number of DHS Major IT Acquisition Programs Reporting Specific IV&V Activities



Source: GAO analysis of DHS data.

Note: This table reflects self-reported data for 35 programs. Seven programs reported other activities not included in this list.

To accomplish IV&V activities, program officials reported obtaining expertise from several different sources: commercial firms, federally funded research and development centers, internal resources, and other federal agencies. Some programs reported obtaining IV&V services from multiple sources. (For further information reported by DHS about the programs and their IV&V efforts, see app. II.)

DHS Has Not Consistently Applied Key Elements of Effective IV&V on Selected Programs

Despite DHS's reported widespread use of IV&V, the eight programs selected for our review did not consistently implement the elements of effective IV&V.[24] These programs—ACE, TASC,[25] ITP, TECS-Mod, NCPS, ITIP, C4ISR, and Transformation—all reported that they planned and performed IV&V on system development and/or acquisition activities

[24]We selected one program to study from each DHS component that reported having a level 1 IT acquisition involving IV&V activities. Our criteria for selecting the programs are described in appendix I. The programs and our evaluation with respect to key elements of IV&V are described in detail in appendix IV.

[25]In May 2011, a DHS official stated that TASC would be cancelled.

throughout their respective program life cycles, at a total estimated cost of about $91 million. (See app. III for a description of the IV&V efforts and costs of these programs, as reported by DHS.) However, our review of documents and artifacts for these programs determined that, in most cases, there were gaps in their implementation of IV&V. Notably, one program—NCPS—demonstrated almost none of the elements of IV&V leading practices. Table 4 summarizes the extent to which each program implemented key elements of effective IV&V. A high-level discussion of implementation across the programs, with selected examples, follows the table. Appendix IV provides the detailed results of our analysis.

Table 4: Summary of DHS's Implementation of IV&V Elements on Eight Large IT Acquisitions

IV&V elements	Program							
	ACE	TASC	ITP	TECS-Mod	NCPS	ITIP	C4ISR	Transformation
Establish risk-based decision criteria	◐	◐	◐	◐	○	◐	○	○
Establish standards for independence	◐	◐	◐	◐	◐	◐	◐	◐
Define the scope of the effort	◐	◐	●	◐	○	◐	◐	◐
Determine the resources that will be required	◐	◐	○	◐	○	○	◐	●
Establish program oversight	◐	◐	◐	◐	○	◐	◐	◐

Source: GAO analysis of DHS data.

Key:

● The program provided evidence that fully satisfied all aspects of this element.

◐ The program provided evidence that satisfied some, but not all, aspects of this element.

○ The program provided evidence that did not satisfy any aspects of this element, or provided no evidence.

- *Decision criteria.* None of the eight programs had fully established decision criteria to guide their IV&V efforts. The five programs that partially met our criteria determined how or when to apply IV&V results to improve the program's management, but they did not establish and use a risk-based approach for deciding whether or to what extent to use IV&V. For example, TASC officials told us that they meet weekly to review key findings and determine how they can improve the management of the program, but that they did not follow a structured, risk-based process in deciding to use IV&V. The remaining three programs did not incorporate either of these aspects into their program decision processes.

- *Standards for independence.* Each of the programs at least partially addressed the independence of their IV&V agents, but none of them ensured full technical, managerial, and financial independence. For

example, TECS-Mod requires that the IV&V contractor provide written certification of its technical, managerial, and financial independence, but the effort is not managerially independent because, according to officials, the contractor is overseen by the TECS-Mod program manager. In another example, the statement of work for Transformation's IV&V effort requires the agent to be technically independent, but it does not address financial or managerial independence.

- *Defined scope of the effort.* Almost all of the programs defined the scope of their IV&V effort to at least some degree. However, only one fully defined its scope. ITP's IV&V plan describes activities subject to IV&V in the concept, requirements, design, and testing phases of the program and includes V&V compliance criteria for all its IV&V activities. Six programs partially defined their scope. Although they defined and documented their IV&V activities, they did not define the related compliance criteria for all activities. For example, the Transformation program identified 15 tasks the IV&V agent is to perform, such as reviewing requirements management and test and evaluation activities, but it did not define all of the required compliance criteria for these tasks. The eighth program—NCPS—did not address either aspect of scope. It documented a high-level description of desired IV&V services, but it did not define the specific activities to be performed or the related evaluation compliance criteria.

- *Required program resources.* Just over half of the programs defined the resources required for their IV&V effort to at least some degree. However, only one fully defined them. Transformation identified the personnel needs, facilities, and tools that were needed to support its IV&V activities, for example, by listing certification requirements for personnel. On the other hand, the C4ISR's IV&V statement of work defined the program's needs for security and test-related activities, but did not define its resource needs for other planned IV&V activities, such as cost estimation and performance verification. Three programs did not specify the resources required for their efforts.

- *Management and oversight.* Seven of the eight programs established some degree of management and oversight for their efforts, although each contained gaps. For example, ACE's IV&V plan and the statement of work note that the agent is to report its results to the program, but do not identify a process for how ACE will respond to such issues. In addition, the responsibilities of ACE's agent are defined; however, the roles and responsibilities for government

officials and evaluating the effectiveness of the IV&V effort were not specified.

These weaknesses in IV&V efforts can be partly attributed to the fact that DHS's acquisition policy does not require that programs apply recognized practices to their IV&V efforts. Performing IV&V without an established framework for planning and managing the effort could result in duplicative, unnecessary, or potentially ineffective IV&V efforts. As a result, DHS risks not maximizing the value of its investment in IV&V, in turn making it less likely that IV&V will contribute significantly toward meeting the schedule and mission goals of its major IT acquisition programs.

Conclusions

DHS spends billions of dollars on large IT acquisitions in support of its national security mission, including millions on independent reviews of these programs. Investment in IV&V by a large number of these programs reflects a view across DHS that it is a worthwhile acquisition practice, a view also represented in DHS's acquisition policy. However, because DHS has not provided guidance for planning, executing, and overseeing the elements of this practice across the department nor required its components to do so, it lacks consistent approaches and criteria for determining whether and how to proceed with IV&V on programs, specifying the needed independence of agents, defining the scope of efforts, planning and procuring the needed resources, and managing and utilizing results.

Not surprisingly, none of the high-budget acquisition programs that we reviewed had fully implemented the key elements of effective IV&V. Executing such efforts without a disciplined framework for planning and management may make such efforts duplicative, unnecessary, or unusable. Moreover, without well-defined mechanisms for tracking IV&V efforts, results, and effectiveness, and incorporating this information into the department's investment management processes, DHS's investment decisions may not adequately take into account the concerns raised by these efforts. To realize IV&V's promise as a tool for reducing the risks inherent in developing IT systems, DHS needs to promote a common understanding of effective IV&V across the department, and through its oversight activities, ensure that component agencies and their large IT programs conduct efforts that consistently contribute toward meeting IT acquisition cost, schedule, and mission goals.

Recommendations for Executive Action

To help guide consistent and effective execution of IV&V at DHS, we recommend that the Secretary of Homeland Security direct the department CIO and CPO to take the following three actions:

- Revise DHS acquisition policy such that it establishes
  - risk-based criteria for (1) determining which major and other high-risk IT acquisition programs should conduct IV&V and (2) selecting appropriate activities for independent review of these programs;
  - requirements for technical, financial, and managerial independence of agents;
  - standards and guidance for defining and documenting plans and products;
  - controls for planning, managing, and overseeing efforts;
  - mechanisms to ensure that plans and significant findings inform DHS acquisition program reviews and decisions, including those of the ARB; and
  - mechanisms to monitor and ensure implementation of this policy on applicable new IT acquisition programs.
- Reevaluate the approach to IV&V for ongoing programs (including the eight programs featured in this report) and ensure that appropriate actions are taken to bring each of them into alignment with the elements of leading practice.
- Collect and analyze data on IV&V efforts for major IT acquisition programs to facilitate the development of lessons learned and evaluation of the effectiveness of DHS's investments, and establish a process that uses the results to inform the department's IT investment decisions.

Agency Comments and Our Evaluation

In written comments on a draft of this report, signed by the Director, Departmental GAO/Office of Inspector General Liaison and reprinted in appendix V, DHS stated that it concurred with our recommendations and described actions planned or under way to address them. Regarding our first recommendation, the department stated that it is drafting an interim IV&V policy implementation plan that will outline best practices, templates, tools, and processes for IV&V. The interim plan will also require programs to

develop IV&V plans early in their life cycle, and to assess programs at their conclusion to ensure that all IV&V artifacts, processes, and systems had been developed properly. Further, the response stated that DHS components will be expected to use the department's implementation plan to tailor IV&V activities based on program size, complexity, risk, and other program management factors. In addition, DHS stated that it is considering modifications to its existing guidance to reflect IV&V industry standards and best practices, and to demonstrate requirements for the independence of IV&V agents as called for in this report. Regarding our second recommendation, the department responded that it is creating an independent team of subject matter experts to provide oversight of IV&V efforts across DHS. This team is to determine whether appropriate resources, tools, and facilities have been allocated, and will report results as necessary. Given the limited extent to which the programs we reviewed are currently employing the key elements of effective IV&V, expeditiously establishing this team and conducting the reviews would help identify the full extent of the need for improvements departmentwide. Concerning our third recommendation, the department's response stated that DHS will create a repository to store data about its IV&V efforts in order to generate lessons learned and gauge the effectiveness of these efforts, among other things. The department also provided technical comments, which we have incorporated in the report, as appropriate.

We are sending copies of this report to the appropriate congressional committees; the Secretary of the Department of Homeland Security; and other interested parties. In addition, this report is available at no charge on our Web site at http://www.gao.gov.

If you or your staff members have any questions on the matters discussed in this report, please contact me at (202) 512-9286 or pownerd@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix VI.

David A. Powner
Director, Information Technology
Management Issues

Appendix I: Objectives, Scope, and Methodology

Our objectives were to determine (1) how the Department of Homeland Security's (DHS) independent verification and validation (IV&V) policies and procedures for information technology (IT) acquisitions compare with leading practices and (2) the extent to which DHS has implemented IV&V on its large IT system acquisitions.

To determine how DHS's IV&V policies and procedures for IT acquisitions compare with leading practices, we first identified key elements of leading practices for IV&V. Specifically, we reviewed (1) the Software Engineering Institute's Capability Maturity Model® Integration,[1] focusing on the validation and verification process areas, (2) the Institute of Electrical and Electronics Engineers (IEEE) standard for software verification and validation,[2] (3) the IEEE/ International Organization for Standardization/ International Electrotechnical Commission standard for system life cycle processes,[3] (4) the International Organization for Standardization standard for software life cycle processes,[4] and (5) our prior work.[5] Within these documents, we identified validation, verification, and independence concepts and practices that these sources have in common. We then categorized the concepts and practices into the following key elements of leading practice for IV&V: (1) decision criteria, (2) effort independence, (3) project scope, (4) project resources, and (5) management and oversight.

We also examined how IV&V is used by other federal agencies to provide context for our review of DHS. We selected the additional agencies by identifying those that had the highest average IT spending per investment for fiscal years 2008 to 2010. They are: the Department of Commerce, the Department of Defense, the Department of Energy, the Department of Homeland Security, the Department of Justice, the National Aeronautics

[1]Software Engineering Institute, Capability Maturity Model® Integration for Development, version 1.2 (August 2006).

[2]Institute of Electrical and Electronics Engineers, *IEEE Standard for Software Verification and Validation,* IEEE Std 1012-2004 (New York: N.Y.: June 8, 2005).

[3]Institute of Electrical and Electronics Engineers/ International Organization for Standardization/ International Electrotechnical Commission, *International Standard for Systems and Software Engineering—System Life Cycle Processes,* ISO/IEC 15288-2008 / IEEE Std 15288-2008 (New York: N.Y.: Jan. 31, 2008).

[4]International Organization for Standardization, "Systems and Software Engineering—Software Life Cycle Processes," ISO Standard 12207-2008 (2008-02-01).

[5]See, for example, GAO-10-40.

and Space Administration (NASA), the Social Security Administration, the Department of State, the Department of Transportation, and the Department of Veterans Affairs. We reviewed their policies regarding IV&V and selected examples that were used to illustrate some of the leading IV&V practices that they follow and perform. Specifically, we identified relevant examples from the Department of Justice and NASA.

Next, we held interviews with DHS officials, and gathered and reviewed the department's policy documents related to IV&V.[6] We then compared the policy and procedures with the five key elements of IV&V leading practice. We used the following rules to characterize the extent to which DHS's policies addressed the elements:

- *Met.* DHS provided evidence that fully satisfied all aspects of the element.
- *Partially met.* DHS provided evidence that satisfied some, but not all aspects of the element.
- *Not met.* DHS provided evidence that did not satisfy any aspects of the element or provided no evidence.

To determine the extent to which DHS had implemented IV&V on its large IT system acquisitions, we first collected information on the status and program characteristics of the 53 level 1 and 2 IT acquisitions[7] listed in DHS's Major Acquisitions Oversight List of May 26, 2010. To do so, we requested from program officials their respective program's life cycle approach, estimated acquisition costs, and planned IV&V activities. During our review, 12 programs were defunded, recategorized to level 3 or non-IT, or taken off the oversight list by DHS and therefore were not analyzed for this report. We used the self-reported program data to populate table 5 in appendix II and to select a subset of programs for more detailed analysis of IV&V implementation.

[6]Department of Homeland Security, Acquisition Instruction/Guidebook, 102-01-001, Interim Version 1.9 (Nov. 7, 2008), including Appendix B, "DHS Systems Engineering Life Cycle"; Department of Homeland Security, Acquisition Management Directive, Directive Number 102-01 (Jan. 20, 2010).

[7]Level 1 programs have estimated acquisition costs of over $1 billion; level 2 programs have estimated costs between $300 million and $1 billion.

We used three criteria to identify programs for further study. First, the selected programs were to represent IV&V implementation across a variety of DHS components. Second, the selected programs would be among DHS's largest (level 1). Third, the selected programs would have the highest estimated acquisition cost within each of DHS's components. Thus, we selected the largest program (based on estimated acquisition cost) from each DHS component that reported having at least one level 1 IT acquisition that reported using IV&V—with one exception. Since we have previously issued detailed reports on the Coast Guard's largest program, Rescue 21, we instead selected U.S. Coast Guard's Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) program. Using this approach, we selected the eight IT acquisitions featured in appendixes III and IV.

Next, we collected and analyzed IV&V related documents and information from each of these programs and conducted follow-up interviews with cognizant officials to clarify documentation and elaborate their responses. We then compared these data with key elements of effective IV&V and scored the programs using the previously described scoring methodology.

To assess the reliability of the data that was used to support the findings in the report, we reviewed relevant program and agency documentation to substantiate evidence obtained through interviews with knowledgeable agency officials. We validated that the documents we used in this review were current and officially issued by conferring with DHS and component agency officials in meetings and in the formal exit conference. On this basis, we determined that the data used in this report are sufficiently reliable. We appropriately attributed the sources of data we used throughout this report. This includes sections in which data is self-reported, such as figure 3, table 4, appendix II, and appendix III.

We conducted this performance audit at GAO headquarters in Washington, D.C., from March 2010 to July 2011, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: DHS's Large IT Acquisition Programs and Their Reported Use of IV&V

To characterize the extent to which DHS has implemented IV&V on its large IT acquisitions, DHS department, component, and program officials provided the data in table 5 for the level 1 and level 2 IT acquisition programs listed in the major acquisition oversight list issued by the Under Secretary for Management on May 26, 2010. Of the 41 programs, 35 reported planning, conducting, or completing some type of IV&V activity.

The decision makers for conducting IV&V on these programs—congressional mandate, departmental decision, or others—are summarized in the discussion that follows and in table 6.

Table 5: Self-reported Data Characterizing DHS's Large IT Acquisition Programs and Their Use of IV&V

Dollars in millions

Program	DHS acquisition level	Life cycle cost estimate	Current life cycle phase(s)	IV&V activities (see legend at end of table)	Status of IV&V efforts
U.S. Customs and Border Protection					
Advance Passenger Information System	2	$136	O&M	c,e,g,h,i,j	Under way
Automated Commercial Environment /International Trade Data System	1	$4,544	Mixed	a,b,c,d,e,f,g,h,i,j	Under way
Automated Targeting System Maintenance	2	$402	O&M	a,b,c,d,e,f,g,h,i,j,k	Under way
Non-Intrusive Inspection Systems Program	1	$2,268	Mixed	No IV&V	
SAP	2	$359	O&M	No IV&V	
Secure Border Initiative network[a]	1	$1,357	Mixed	b,c,d,e,g,h,i,k	Under way
Tactical Communication	2	$1,300	Mixed	j	Planned
TECS Modernization	1	$660	Mixed	a,b,c,d,e,f,g,h,i,j	Under way
Western Hemisphere Travel Initiative	1	$2,530	O&M	a,b,c,d,e,f,g,h,i, j	Complete
Federal Emergency Management Agency					
Logistics Supply Chain Management System	2	$363	Mixed	h	Planned
Risk Mapping, Analysis and Planning	1	$3,987	Mixed	b,c,d,e,f,g,i,j	Under way
U.S. Immigration and Customs Enforcement					
Atlas	2	$822	Full	b,c	Complete
Detention and Removal Operations	2	$408	Mixed[b]	a,b,c,d,e,f,g,i,j	Complete

Program	DHS acquisition level	Life cycle cost estimate	Current life cycle phase(s)	IV&V activities (see legend at end of table)	Status of IV&V efforts
DRO Electronic Health Record System	2	Did not respond	Mixed	a,b,c,d,e,f,g,i,j	Complete
Federal Financial Management System	2	$349	O&M[c]	i	Planned
ICE TECS Modernization	1	$818	Mixed	a,b,c,d,e,f,g,h,i,j,k	Planned[d]
Student & Exchange Visitor Information System	2	$249	Mixed	a,b,c,e,f,g,k	Under way
National Protection and Programs Directorate					
IICV (Infrastructure Information Collection Program & Visualization) - Infrastructure Information Collection Program	2	$134	Mixed	f	Under way
National Cybersecurity & Protection System	1	$1,200	Mixed	a,c,d,e,f,h,i	Under way
Next Generation Network	1	$210	Full	a,b,c,d,j	Planned
United States Visitor and Immigrant Status Indicator Technology	1	$8,288	Mixed	a,b,c,d,e,f,g,h,i,j,k	Under way
Office of the Chief Financial Officer					
Transformation and Systems Consolidation	1	$991	Planning	b,c,d,e,f,g,h,i,j	Under way
Office of the Chief Information Officer					
Homeland Secure Data Network	2	$732	O&M	a,b,c,d,e,f,g,i,j	Complete
Infrastructure Transformation Program	1	$1,200	Mixed	a,b,c,d,e,f,g,h,i,j	Complete
Office of Operations Coordination and Planning					
Common Operational Picture	2	$133	Mixed	b,c,d,f,h,i,j,k	Under way
Homeland Security Information Network	2	$451	Mixed	b,c,d,f,h,ij	Under way
Transportation Security Administration					
Information Technology Infrastructure Program	1	$3,500	O&M	a,b,c,f,g,j	Planned
Secure Flight	1	$1,371	O&M	c,f,i,j	Complete
Security Technology Integrated Program	2	$215	Mixed	a,g	Under way
Transportation Worker Identification Credentialing	1	$677	O&M	No IV&V	
Transportation Threat Analysis Center Infrastructure Modernization Program	2	$570	Planning	h,i,j	Planned

Program	DHS acquisition level	Life cycle cost estimate	Current life cycle phase(s)	IV&V activities (see legend at end of table)	Status of IV&V efforts
U.S. Citizenship and Immigration Services					
Benefits Provision - Verification Information System	2	$467	Mixed	a,b,c,d,e,f,g,h,i,j	Under way
Integration Document Production	2	$736	O&M	No IV&V	
Transformation Program	1	$1,700[e]	Planning	a,b,c,d,e,f,g,h,i,j	Under way
U.S. Coast Guard					
CG Logistics Information Management System	2	No approved LCCE	Planning	a,f,j	Planned
C4ISR	1	$1,300	Mixed	a,b,f,h,i,j,k	Under way
Core Accounting System	2	$459	O&M	No IV&V	
Interagency Operations Centers	1	No approved LCCE	Mixed	a,b,c,f,j,k	Under way
Nationwide Automatic Identification System	1	$1,241	Mixed	a,b,c,f,h,i,j	Under way
Rescue 21	1	$2,662	Mixed	a,b,f,h,i,j,k	Under way
U.S. Secret Service					
IT Modernization	2	$0.18	Planning	No IV&V	

Legend for IV&V activities

a=Independent cost estimation or cost estimate validation

b=Program progress or performance verification or evaluation

c=Requirements validation or verification

d=Concept or design validation, verification, or alternatives analysis

e=Risk evaluation

f=Security vulnerability or security risk assessments

g=Configuration management verification

h=Component verification testing and evaluation

i=System or integration verification testing and evaluation

j=Operational readiness testing and evaluation

k=Other

Source: GAO analysis of DHS self-reported data based on DHS's Major Acquisitions Oversight List dated May 26, 2010.

Note: Data presented in this table is current as of May 3, 2011.

[a]In January 2011, the Secretary of Homeland Security directed CBP to end the Secure Border Initiative network program as originally conceived.

[b]"Mixed" life cycle phase means some combination of the other life cycle phases.

[c]"O&M" means operations and maintenance phase.

[d]U.S. Immigration and Customs Enforcement officials stated TECS-Mod has conducted IV&V efforts on the requirement phase of the program and plans to conduct IV&V on future phases of the program.

[e]U.S. Citizenship and Immigration Services Transformation Program life cycle cost estimate is currently under review.

DHS officials also provided information about the origins of their IV&V decisions for these programs. For the 18 level 1 acquisitions that reported IV&V activities, Congress mandated that 2 of the acquisitions perform IV&V; DHS required that 7 of the programs use IV&V; and the component, program, or other entity decided to perform IV&V on 9 of the acquisitions. For the 17 level 2 acquisitions that reported IV&V activities, none were congressionally mandated; DHS required IV&V for 2 of the acquisitions; and component, programs, or other entities decided to perform IV&V on 15 acquisitions. Table 6 summarizes the decision makers for conducting IV&V on level 1 and level 2 programs.

Table 6: DHS and Program Officials' Description of the Origins of Its IV&V Decisions

	Number of acquisitions reporting IV&V efforts	IV&V congressionally mandated	IV&V decision by department	IV&V decision by component, program, or others
Level 1	18	2	7	9
Level 2	17	0	2	15

Source: GAO analysis of DHS and program officials' self-reported data.

Appendix III: Overview of DHS's Reported Use of IV&V on Selected Large IT Acquisitions

Table 7 summarizes key characteristics of eight large DHS IT acquisitions and their associated IV&V efforts and costs, as reported by DHS program officials for this review. The systems engineering life cycle stages identified in the table are further discussed in the context of DHS's acquisition life cycle after the table.

Table 7: Selected DHS Large IT Acquisitions, Their Current Life Cycle Stage(s) and Use of IV&V

Dollars in millions, except where noted

Component or division	Program	Current life cycle stage(s)	Date of department approval	IV&V activities	Life cycle cost estimate (LCCE)	IV&V cost estimate (% of LCCE)
U.S. Customs and Border Protection	Automated Commercial Environment /International Trade Data System	11 segments: Planning (1), Development (2), Operations & Maintenance (8)	3/6/2000	a—j	$4.5 billion	$2.8 (.06%)
Office of the Chief Financial Officer	Transformation and System Consolidation	Solution Engineering	2/10/2009	b—j	$991	$3.4 (0.3%)
Office of the Chief Information Officer	Infrastructure Transformation Project	4 segments: Planning (1), Operations & Maintenance (3)	7/31/2005	a—j	$1.2 billion	No estimate provided
U.S. Immigration and Customs Enforcement	TECS-Modernization	Requirements definition	7/1/2007	a—k	$818 (total program $1.1 billion)	$1.75 (0.2%)
National Protection and Programs Directorate	National Cybersecurity Protection System	5 segments: Planning (1), Design (1), Integration (1), Operations & Maintenance (2)	2/27/2009	a,c,d,e,f,h,i	$1.2 billion	$0.5 (0.04%)
Transportation Security Administration	Information Technology Infrastructure Program	Operations & Maintenance	2/1/2002	a,b,c,f,g,j	$3.5 billion	No estimate provided
U.S. Coast Guard	C4ISR	Development	11/6/2006	a,b,f,h,i,j	$1.3 billion	$20.6 (1.6%)
U.S. Citizenship and Immigration Services	Transformation Program	5 segments: Planning (4), Requirements Definition (1)	11/1/2005	a—j	$1.7 billion[a]	$62 (3.6%)

Legend for IV&V activities

a=Independent cost estimation or cost estimate validation

b=Program progress or performance verification or evaluation

c=Requirements validation or verification

d=Concept or design validation verification, or alternatives analysis

e=Risk evaluation

f=Security vulnerability or security risk assessments

g=Configuration management verification

h=Component verification testing and evaluation

i=System or integration verification testing and evaluation

j=Operational readiness testing and evaluation

k=Software design/development RFP

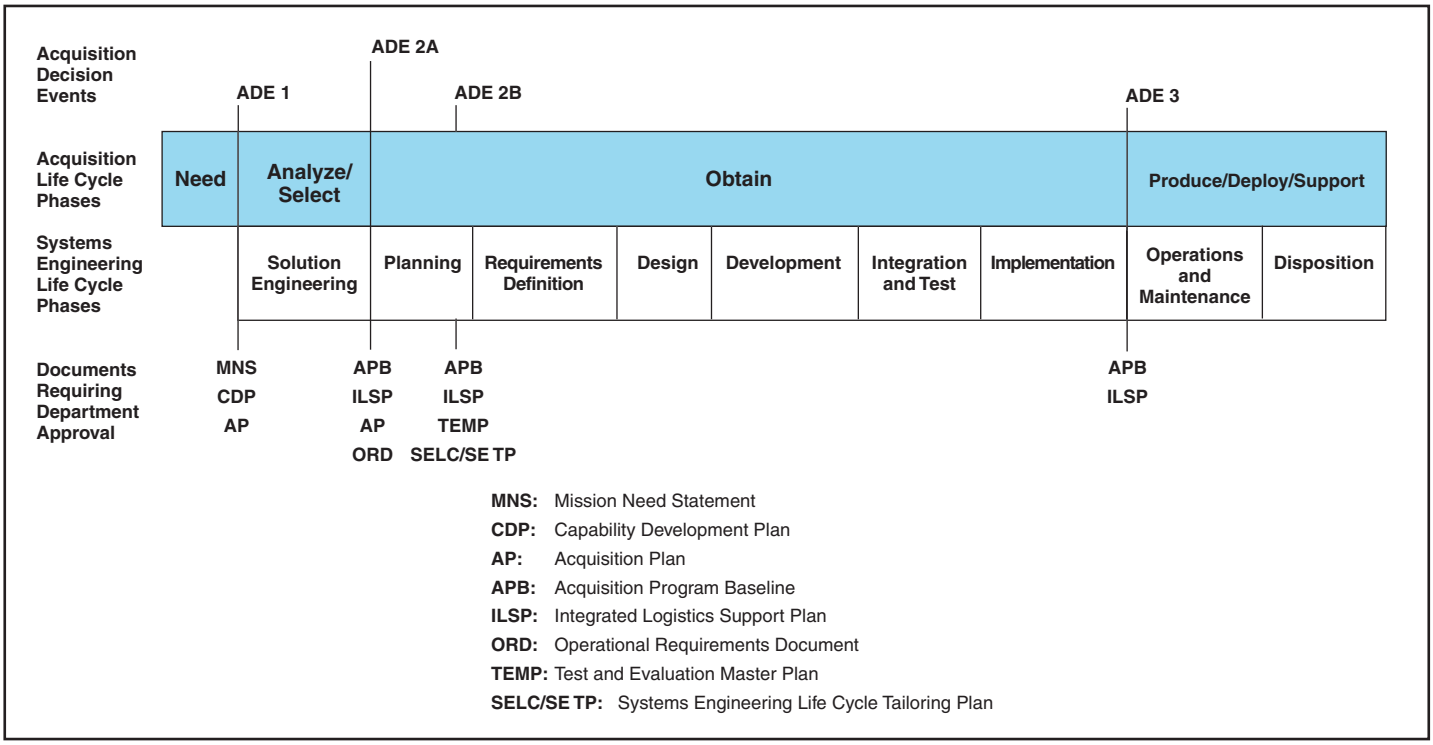
Source: GAO analysis of DHS data.

[a]USCIS Transformation Program LCCE is currently under review.

DHS's Acquisition Instruction/Guidebook establishes a four-phase acquisition life cycle. These life cycle phases are: (1) identify a capability need; (2) analyze and select the means to provide that capability; (3) obtain the capability; and (4) produce, deploy, and support the capability. These phases generally align with one or more systems engineering life cycle phases.

The directive requires the Acquisition Review Board (ARB) to review each major acquisition program at least three times at key Acquisition Decision Events during a program's acquisition life cycle. Selected documents considered during Acquisition Decision Events, such as the mission need statement, the acquisition plan, and the integrated logistics support plan, are depicted in the following figure, along with the associated systems engineering life cycle phases.

Figure 4: The Acquisition Life Cycle, Systems Engineering Life Cycle and Key Acquisition Documents at DHS



Source: DHS Acquisition Instruction/Guidebook 102-01-001, interim, version 1.9, Nov. 7, 2008.

Appendix IV: Assessments of Selected Programs' Implementation of IV&V

This appendix presents brief program overviews and our assessment of DHS's implementation of IV&V on eight select large IT acquisitions compared with key elements of effective IV&V.

U.S. Customs and Border Protection (CBP)—Automated Commercial Environment (ACE)/ International Trade Data System

ACE is a commercial trade processing system intended to facilitate the movement of legitimate trade, strengthen border security, and replace existing systems with a single system for collecting and providing trade data to federal agencies. It is a level 1 acquisition with a life cycle cost of approximately $4.5 billion. Of the total life cycle cost, approximately $2.8 million has been budgeted for IV&V. ACE has been divided into 11 segments, consisting of one in the planning stage, two in the development stage, and eight in the operations and maintenance stage.

ACE officials reported that the following IV&V activities are under way or planned:

- independent cost estimation or cost estimate validation;
- program progress or performance verification or evaluation;
- requirements validation or verification;
- concept or design validation, verification, or alternatives analysis;
- risk evaluation;
- security vulnerability or security risk assessment;
- configuration management verification;
- component verification testing and evaluation;
- system or integration verification testing and evaluation; and
- operational readiness testing and evaluation.

Table 8 describes the extent to which ACE has implemented the key elements of effective IV&V.

Table 8: ACE's Implementation of the Key Elements of Effective IV&V

Key element	Summary of implementation
Decision criteria. A risk-based, decision-making process is defined to determine whether or the extent to which programs should be subject to IV&V, to include (1) establishing risk-based criteria for determining which programs should be subject to IV&V; and (2) establishing a process for using IV&V to improve the management of the IT acquisition/development program.	*Partially met.* The decision to implement IV&V for ACE was based on a conclusion that the program had a high risk of failure; however, specific risk-based criteria were not established or used in the decision to conduct IV&V. In addition, while ACE's IV&V plan requires that the contractor identify and provide recommendations for improvements, it does not include a process for reviewing or implementing improvements or recommendations.
IV&V effort independence. The degree of technical, managerial, and financial independence required of the personnel or agents performing IV&V is defined, including (1) technical, managerial, and financial independence requirements for the IV&V agent; and (2) a mechanism for reporting the results of IV&V to program oversight officials, as well as program management.	*Partially met.* ACE's IV&V plan states that technical, managerial, and financial independence are all essential, and IV&V is performed by an agent independent from the program. However, the IV&V plan does not specifically describe how the program ensures the technical, managerial, or financial independence of the IV&V agent. It has also identified a mechanism for reporting IV&V results to program management officials, but not to program oversight officials.
IV&V program scope. The scope of IV&V activities is defined, including (1) a definition of the program activities subject to IV&V; and (2) validation and verification compliance criteria for each program activity subject to IV&V.	*Partially met.* ACE's IV&V plan identifies activities to be conducted by the IV&V team, such as reviewing requirements development, and test and evaluation activities. Also, the statement of work also identifies deliverables that are to be submitted, such as weekly status reports. However, the program office stated that several other IV&V activities are performed internally by subject matter experts, but that this work is not defined in formal plans. ACE has also not defined the criteria that the IV&V agent is to use as a basis for assessing program activities or measuring compliance.
IV&V program resources. The resources needed for IV&V are specified, including (1) the facilities, personnel, tools, and techniques and methods.	*Partially met.* ACE's IV&V statement of work identifies several program resource needs, such as personnel requirements and a methodology for conducting assessments. However, several other IV&V activities performed internally by subject matter experts are not defined in formal plans.
IV&V management and oversight. The management and oversight to be performed are specified, including (1) the process for responding to issues raised by the IV&V effort; (2) the roles and responsibilities of all parties involved in the program; and (3) how the effectiveness of the IV&V effort will be evaluated.	*Partially met.* ACE's IV&V plan and the IV&V statement of work note that the contractor is to report its results, but they do not identify a process for responding to the issues. The responsibilities of the IV&V contractor are defined in an IV&V plan and also in the associated statement of work. However, ACE has not identified the IV&V roles and responsibilities of government officials. Furthermore, ACE requires that IV&V contractors provide objective evidence that their analyses and recommendations for improvements are well-supported but does not identify how the program will evaluate the effectiveness of the IV&V effort in identifying such improvements.

Source: GAO analysis of DHS data.

Office of the Chief Financial Officer—Transformation and System Consolidation (TASC) Program

TASC was announced in 2007 and is intended to modernize, transform, and integrate the various financial acquisition and asset management systems in use at the department's components.[1] It is a level 1 acquisition and has a life cycle cost estimate of approximately $991 million, with $3.4 million budgeted for IV&V.

TASC reported that it was in the solutions engineering phase of its life cycle and that IV&V is planned or under way in the following activities:

- program progress or performance verification or evaluation;
- requirements validation or verification;
- concept or design validation verification, or alternatives analysis;
- risk evaluation;
- security vulnerability or security risk assessments;
- configuration management verification;
- component verification testing and evaluation;
- system or integration verification testing and evaluation; and
- operational readiness testing and evaluation.

Table 9 describes the extent to which the program has implemented the key elements of effective IV&V.

[1]In May 2011, a DHS official stated that TASC would be cancelled.

Table 9: TASC's Implementation of the Key Elements of Effective IV&V

Key element	Summary of implementation
Decision criteria. A risk-based, decision-making process is defined to determine whether or the extent to which programs should be subject to IV&V, to include (1) establishing risk-based criteria for determining which programs should be subject to IV&V; and (2) establishing a process for using IV&V to improve the management of the IT acquisition/development program.	*Partially met.* TASC officials stated that they did not follow a structured, risk-based process to make IV&V decisions, but that IV&V decisions were made based on their view that IV&V is a best practice. TASC also has not documented a process for using IV&V to improve IT program management. However, TASC officials stated that they meet weekly with officials from the Office of the Chief Information Officer and the Office of the Chief Financial Officer to review, among other things, key IV&V findings and how they can improve the management of the program.
IV&V effort independence. The degree of technical, managerial, and financial independence required of the personnel or agents performing IV&V is defined, including (1) technical, managerial, and financial independence requirements for the IV&V agent; and (2) a mechanism for reporting the results of IV&V to program oversight officials, as well as program management.	*Partially met.* TASC officials have documented the degree of technical, managerial, and financial independence required for IV&V agents. To ensure technical independence, TASC's IV&V agents sign conflict of interest clauses in the IV&V statement of work that exclude them from performing development work and require that they disclose any actual or potential conflicts of interest. Regarding managerial independence, IV&V agents present reports to both the Office of the Chief Information Officer and Office of the Chief Financial Officer and can also raise issues to DHS's Undersecretary for Management. For financial independence, the Office of the Chief Information Officer provides a Contracting Officer's Technical Representative unrelated to the program to manage the IV&V work and oversee the associated funding. TASC officials stated that they have a process for presenting key IV&V findings to officials from the Office of the Chief Information Officer and Office of the Chief Financial Officer, as well as the program Risk Review Board; however, this process is not documented, and TASC did not provide evidence that the process has been implemented.
IV&V program scope. The scope of IV&V activities is defined, including (1) a definition of the program activities subject to IV&V; and (2) validation and verification compliance criteria for each program activity subject to IV&V.	*Partially met.* TASC's IV&V statement of work defines the activities that IV&V agent is to perform. However, Office of the Chief Financial Officer did not present evidence of validation and verification compliance criteria.
IV&V program resources. The resources needed for IV&V are specified, including (1) the facilities, personnel, tools, and techniques and methods.	*Partially met.* TASC's IV&V statement of work provides some information on facilities, personnel, and tools. For example, for IV&V tasks, methods, and deliverables are outlined, including personnel that are responsible for the various reports. However, it does not address funding.
IV&V management and oversight. The management and oversight to be performed are specified, including (1) the process for responding to issues raised by the IV&V effort; (2) the roles and responsibilities of all parties involved in the program; and (3) how the effectiveness of the IV&V effort will be evaluated.	*Partially met.* According to officials, TASC has a process for responding to issues raised by the IV&V effort that includes escalating issues to the Undersecretary of Management, if needed, but this process has not been documented. In addition, while the IV&V agent's responsibilities are defined within the IV&V statement of work, TASC officials stated the department's roles and responsibilities are not yet formally documented. Finally, TASC does not have a process in place to evaluate the effectiveness of the program's IV&V effort. Program officials review activities to see if they are meeting criteria; however, they have not defined how they measure the effectiveness of the IV&V effort.

Source: GAO analysis of DHS data.

Office of the Chief Information Officer—Infrastructure Transformation Program (ITP)

ITP is intended to contribute to DHS's consolidated infrastructure investment, supporting areas such as data center, network, and e-mail consolidation. With a life cycle cost of approximately $1.2 billion, ITP is a level 1 acquisition. The program has four segments; one segment is in the planning stage, and three are in the operations and maintenance phase.

Officials from the Office of the Chief Information Officer report that the IV&V agent for ITP is currently performing the following program activities:

- independent cost estimation or cost estimate validation;
- program progress or performance verification or evaluation;
- requirements validation or verification;
- concept or design validation verification, or alternatives analysis;
- risk evaluation;
- security vulnerability or security risk assessments;
- configuration management verification;
- component verification testing and evaluation;
- system or integration verification testing and evaluation; and
- operational readiness testing and evaluation.

Table 10 describes the extent to which the program has implemented the key elements of effective IV&V.

Table 10: ITP's Implementation of the Key Elements of Effective IV&V

Key element	Summary of implementation
Decision criteria. A risk-based, decision-making process is defined to determine whether or the extent to which programs should be subject to IV&V, to include (1) establishing risk-based criteria for determining which programs should be subject to IV&V; and (2) establishing a process for using IV&V to improve the management of the IT acquisition/development program.	*Partially met.* The decision by the Office of the Chief Information Officer to perform IV&V on ITP was not based on risk-based criteria. Officials stated that the IV&V decision was based upon their belief that IV&V is a best practice for system engineering and program management, and because it provides objective assessments of a program's processes, products, and risks. In addition, the ITP IV&V plan requires findings to be reported to key stakeholders. However, ITP does not have a documented process for using IV&V to improve the management of the program.
IV&V effort independence. The degree of technical, managerial, and financial independence required of the personnel or agents performing IV&V is defined, including (1) technical, managerial, and financial independence requirements for the IV&V agent; and (2) a mechanism for reporting the results of IV&V to program oversight officials, as well as program management.	*Partially met.* ITP's IV&V plan states that a qualified IV&V contractor will be selected using a competitive procurement process, but it does not define the degree of technical, managerial, and financial independence that are required. The IV&V plan also states IV&V results are to be reported to oversight officials and program management; however, it does not describe the mechanism for reporting the results.
IV&V program scope. The scope of IV&V activities is defined, including (1) a definition of the program activities subject to IV&V; and (2) validation and verification compliance criteria for each program activity subject to IV&V.	*Met.* ITP has defined several program activities that will be subject to IV&V across the acquisition life cycle. For example, the ITP IV&V Plan describes activities subject to IV&V in the concept, requirements, design, and testing phases of the program. ITP's IV&V plan also describes validation and verification compliance criteria for all its IV&V activities, including, requirement assessments, design evaluation, test plan analysis, and documentation reviews.
IV&V program resources. The resources needed for IV&V are specified, including (1) the facilities, personnel, tools, and techniques and methods.	*Not met.* ITP's IV&V plan does not identify the resources required for IV&V.
IV&V management and oversight. The management and oversight to be performed are specified, including (1) the process for responding to issues raised by the IV&V effort; (2) the roles and responsibilities of all parties involved in the program; and (3) how the effectiveness of the IV&V effort will be evaluated.	*Partially met.* ITP's IV&V plan requires IV&V findings to be reported to executive management. Additionally, the plan states that the program control office will monitor progress in addressing issues identified by the IV&V agent. However, the specific process for responding to the IV&V findings was not documented. ITP's IV&V plan includes roles and responsibilities for the IV&V agent, but roles and responsibilities for program officials or others involved with the IV&V findings are not defined. In addition, the plan does not describe how the effectiveness of the IV&V effort will be evaluated.

Source: GAO analysis of DHS data.

U.S. Immigration and Customs Enforcement (ICE)—TECS Modernization (TECS-Mod)

TECS-Mod is intended to modernize the system ICE uses to perform investigative activities. Specifically, TECS-Mod involves modernizing the investigative case management system and related support modules of the legacy TECS system. ICE's total combined life cycle cost is estimated at approximately $1.1 billion and an estimated $1.75 million for IV&V efforts.

The program is a level 1 acquisition and is currently in the requirements definition phase. According to ICE officials, the IV&V agents for TECS-Mod are to perform the following IV&V activities:

- independent cost estimation or cost estimate validation;
- program progress or performance verification or evaluation;
- requirements validation or verification;
- concept or design validation, verification, or alternatives analysis;
- risk evaluation;
- security vulnerability or security risk assessments;
- configuration management verification;
- component verification testing and evaluation;
- system or integration verification testing and evaluation;
- operational readiness testing and evaluation; and
- software design and development request for proposals.

Table 11 describes the extent to which the program has implemented the key elements of effective IV&V.

Table 11: TECS-Mod's Implementation of the Key Elements of Effective IV&V

Key element	Summary of implementation
Decision criteria. A risk-based, decision-making process is defined to determine whether or the extent to which programs should be subject to IV&V, to include (1) establishing risk-based criteria for determining which programs should be subject to IV&V; and (2) establishing a process for using IV&V to improve the management of the IT acquisition/development program.	*Partially met.* According to ICE officials, the program manager and chief information officer decided to implement IV&V, but they did not use risk-based criteria and did not document the rationale for their decision. Going forward, however, ICE has identified a set of criteria for deciding whether to use IV&V on future programs, which include the program's size, strategic importance, and other concerns. Further, ICE's IV&V Program Assessment Management Plan identifies planned steps for using IV&V to improve management of the program, such as requiring having the program manager and the Office of the Chief Information Officer Executive Board to review the IV&V team's recommendations. However, it currently does not have this process documented and stated that it is working on a plan to do so.
IV&V effort independence. The degree of technical, managerial, and financial independence required of the personnel or agents performing IV&V is defined, including (1) technical, managerial, and financial independence requirements for the IV&V agent; and (2) a mechanism for reporting the results of IV&V to program oversight officials, as well as program management.	*Partially met.* The TECS-Mod IV&V statement of work notes the importance of independence and requires that the IV&V contractor provide written certification of its technical, managerial, and financial independence. However, as implemented, there is a lack of technical and managerial independence because, according to ICE officials, the IV&V agent is managed and overseen by the ICE TECS-Mod program manager. Further, ICE was not able to provide a document that describes financial independence for the IV&V effort. In addition, the TECS-Mod IV&V task order identifies the mechanism for reporting IV&V results and states that a report is to be developed for each review area and reported to the program manager. However, it does not identify a mechanism for reporting to program oversight officials.
IV&V program scope. The scope of IV&V activities is defined, including (1) a definition of the program activities subject to IV&V; and (2) validation and verification compliance criteria for each program activity subject to IV&V.	*Partially met.* TECS-Mod's IV&V statement of work and task order define program activities subject to IV&V. For example, IV&V is to include a review of risk evaluation, configuration management, and test-related activities. The task order also establishes validation and verification compliance criteria for one IV&V activity (assessing the performance of the program's procurement process). However, it did not include criteria for any other IV&V activities.
IV&V program resources. The resources needed for IV&V are specified, including (1) the facilities, personnel, tools, and techniques and methods.	*Partially met.* TECS-Mod's IV&V statement of work identifies some personnel resource needs, including the amount and types of key personnel. It also identifies certain tools to be used; states that the IV&V agent is to have access to facilities needed to carry out its work; and describes methodologies to be followed, such as the Software Engineering Institute's methodologies for development and for acquisition. However, it does not contain specific descriptions of the facilities, techniques, and methods required to perform the individual assessments.

Key element	Summary of implementation
IV&V management and oversight. The management and oversight to be performed are specified, including (1) the process for responding to issues raised by the IV&V effort; (2) the roles and responsibilities of all parties involved in the program; and (3) how the effectiveness of the IV&V effort will be evaluated.	*Partially met*. TECS-Mod officials reported that the contractor submits IV&V recommendations to the program manager, and a database is maintained with the status of actions taken on each recommendation, as called for in the ICE IV&V Program Assessment Management Plan. Officials also provided a sample report which identified IV&V recommendations, their priority and their status (i.e., in progress or recommended for closure). Further, the IV&V contractor's responsibilities, including the tasks and deliverables, are detailed in a statement of work and task order. The statement of work also describes government responsibilities with respect to furnishing equipment, and the ICE IV&V Program Assessment Management Plan describes roles and responsibilities for government officials. However, officials reported that they are working on a transition strategy to implement the management plan. Finally, the TECS-Mod statement of work requires that the IV&V agent develop and submit work plans and progress reports that are to be used in determining its performance against milestones, major accomplishments, as well as identifying risks and issues. However, officials did not demonstrate that they use these measures to actually evaluate the effectiveness of the IV&V activities. Also, ICE's Program Assessment Management Plan identifies potential measures that may be used to evaluate the IV&V effort, such as the percentage of IV&V recommendations implemented, whether there are fewer problems identified during testing, and whether staff perceptions of the IV&V program have improved. However, officials reported that they are working on a transition strategy to implement these measures.

Source: GAO analysis of DHS data.

National Protection and Programs Directorate (NPPD)—National Cybersecurity Protection Systems (NCPS)

The NCPS program is intended to reduce the federal government's vulnerabilities to cyber threats by decreasing the frequency of cyberspace disruptions and minimizing the duration and damage of those disruptions. It is classified as a level 1 acquisition with a total estimated life cycle cost of approximately $1.2 billion. The program is structured in five segments, three of which are under development—one in the planning stage, one in design, and one in integration. Two segments have been completed and are in the operations and maintenance phase.

NPPD officials reported that the following IV&V activities are either planned, under way, or have been completed:

- independent cost estimation or cost estimate validation;
- requirements validation or verification;
- concept or design validation, verification, or alternatives analysis;
- risk evaluation;

- security vulnerability or security risk assessments;
- component verification testing and evaluation; and
- system or integration verification testing and evaluation.

Table 12 describes the extent to which the program has implemented the key elements of effective IV&V.

Table 12: NCPS's Implementation of the Key Elements of Effective IV&V

Key element	Summary of implementation
Decision criteria. A risk-based, decision-making process is defined to determine whether or the extent to which programs should be subject to IV&V, to include (1) establishing risk-based criteria for determining which programs should be subject to IV&V; and (2) establishing a process for using IV&V to improve the management of the IT acquisition/development program.	*Not met.* The decision to use IV&V on NCPS was not based on risk-based criteria. Instead, officials stated that in late 2008 program management recognized the need for IV&V, which they regard as a best practice. The program's acquisition strategy documented a formal intention to award an IV&V contract. NCPS also does not have documented policies or procedures for using IV&V to improve acquisition management. Program officials stated that IV&V is intended to provide an independent assessment of the quality of program execution and the opportunity for more effective program decision making. Nevertheless, NCPS does not have a defined process for how IV&V will be used to achieve program improvements.
IV&V effort independence. The degree of technical, managerial, and financial independence required of the personnel or agents performing IV&V is defined, including (1) technical, managerial, and financial independence requirements for the IV&V agent; and (2) a mechanism for reporting the results of IV&V to program oversight officials, as well as program management.	*Partially met.* For technical independence, NCPS officials stated that they use IV&V contractors who do not have a role in the portion of the program they are reviewing. For financial independence, NCPS officials said that Cost Estimation and Security Vulnerability reviews were funded by nonprogram funds and executed out of a separate DHS office. However, officials did not provide documentation on how technical and financial independence is ensured and they did not address managerial independence at all. NCPS also does not have a documented process for reporting the results of IV&V to program oversight officials or program management.
IV&V program scope. The scope of IV&V activities is defined, including (1) a definition of the program activities subject to IV&V; and (2) validation and verification compliance criteria for each program activity subject to IV&V.	*Not met.* The NCPS acquisition strategy contains a short, high-level description of IV&V services, but it does not provide details on the tasks to be performed. It also does not establish compliance criteria for each of the program activities that will be subject to IV&V.
IV&V program resources. The resources needed for IV&V are specified, including (1) the facilities, personnel, tools, and techniques and methods.	*Not met.* NCPS does not specify the resources required for the IV&V effort. The NCPS acquisition strategy states that the IV&V contractor is to provide best practices, technologies, tools, and support to quality and operational assessments, integration testing, and system test and evaluation, including security certification and accreditation, for IT systems, but it does not identify these resources, and does not explain the facilities, personnel, techniques, and methods to be utilized.

Key element	Summary of implementation
IV&V management and oversight. The management and oversight to be performed are specified, including (1) the process for responding to issues raised by the IV&V effort; (2) the roles and responsibilities of all parties involved in the program; and (3) how the effectiveness of the IV&V effort will be evaluated.	*Not met.* NCPS has not defined a process for responding to issues raised by the IV&V effort. In addition, officials stated that roles and responsibilities for IV&V are not documented at this time. They stated that IV&V responsibilities assigned to staff are consistent with existing program office practices, and they intend to formalize IV&V roles in the future. Finally, it does not have a process for evaluating the effectiveness of its IV&V efforts.

Source: GAO analysis of DHS data.

Transportation Security Administration (TSA)—Information Technology Infrastructure Program (ITIP)

ITIP is intended to provide comprehensive technical infrastructure support for TSA in four main program areas: (1) office automation, (2) infrastructure, (3) program management, and (4) contract support. It is a level 1 acquisition, with a life cycle cost of approximately $3.5 billion. ITIP is currently in operations and maintenance.

ITIP officials reported that the following IV&V activities are under way:

- independent cost estimation or cost estimate validation;
- program progress or performance verification or evaluation;
- requirements validation or verification;
- security vulnerability or security risk assessments;
- configuration management verification; and
- operational readiness testing and evaluation.

Table 13 describes the extent to which the program has implemented the key elements of effective IV&V.

Table 13: ITIP's Implementation of the Key Elements of Effective IV&V

Key element	Summary of implementation
Decision criteria. A risk-based, decision-making process is defined to determine whether or the extent to which programs should be subject to IV&V, to include (1) establishing risk-based criteria for determining which programs should be subject to IV&V; and (2) establishing a process for using IV&V to improve the management of the IT acquisition/development program.	*Partially met*. TSA did not use a risk-based approach to determine whether, or the extent to which, IV&V should be performed on ITIP. Instead, officials told us that program management made the decision to use IV&V, but the basis of the decision was not documented. In addition, TSA's Performance Management and Incentive Process documents a process for using IV&V to improve the management of ITIP by measuring the accuracy and validity of performance data. The document did not contain evidence that other IV&V activities are considered when improving the management of the IT acquisition.
IV&V effort independence. The degree of technical, managerial, and financial independence required of the personnel or agents performing IV&V is defined, including (1) technical, managerial, and financial independence requirements for the IV&V agent; and (2) a mechanism for reporting the results of IV&V to program oversight officials, as well as program management.	*Partially met.* TSA officials stated that IV&V agents are independent because they are a third party. However, TSA has not defined or implemented controls to ensure that its IV&V agents possess an appropriate degree of technical, managerial, or financial independence. TSA's Performance Management and Incentive Process document does not have a mechanism for reporting IV&V results to program oversight authorities.
IV&V program scope. The scope of IV&V activities is defined, including (1) a definition of the program activities subject to IV&V; and (2) validation and verification compliance criteria for each program activity subject to IV&V.	*Partially met.* TSA's Performance Management and Incentive Process document contains the definition of one of the six the program activities that are subject to IV&V—performance verification. It does not address the other five activities. In addition, the Performance Management and Incentive Process compliance document only contains criteria for one IV&V activity outlined in ITIP's statement of work—the infrastructure build-out performance standard is based on the percent of contractor proposals that do not require additional clarification or comment from the government. Other IV&V activities are not addressed.
IV&V program resources. The resources needed for IV&V are specified, including (1) the facilities, personnel, tools, and techniques and methods.	*Not met*. TSA did not define the resources required for performing the IV&V effort.
IV&V management and oversight. The management and oversight to be performed are specified, including (1) the process for responding to issues raised by the IV&V effort; (2) the roles and responsibilities of all parties involved in the program; and (3) how the effectiveness of the IV&V effort will be evaluated.	*Partially met.* TSA officials did not provide a documented process for responding to issues raised by ITIP's IV&V effort. In addition, TSA has defined IV&V roles and responsibilities for the IV&V agent, and identified two job titles for government officials involved with IV&V in its Performance Management and Incentive Process. However, responsibilities for government personnel were not documented. Finally, TSA officials did not provide documentation that defines how the effectiveness of the IV&V effort will be evaluated.

Source: GAO analysis of DHS data.

U.S. Coast Guard (USCG)—Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR)

USCG's C4ISR program is intended to be an interoperable network that combines information from USCG assets and sensors, allowing the USCG to see, comprehend, and communicate rapidly. It is a level 1 acquisition with a life cycle cost of approximately $1.3 billion (according to its 2011 budget submission) and is currently in the development phase. Of this cost, about $20.6 million is budgeted for IV&V.

USCG officials report that the IV&V agent is performing the following IV&V activities:

- independent cost estimation or cost estimate validation;
- program progress or performance verification or evaluation;
- security vulnerability or security risk assessments;
- component verification testing and evaluation;
- system or integration verification testing and evaluation; and
- operational readiness testing and evaluation.

Table 14 describes the extent to which the program has implemented the key elements of effective IV&V.

Table 14: C4ISR's Implementation of the Key Elements of Effective IV&V

Key element	Summary of implementation
Decision criteria. A risk-based, decision-making process is defined to determine whether or the extent to which programs should be subject to IV&V, to include (1) establishing risk-based criteria for determining which programs should be subject to IV&V; and (2) establishing a process for using IV&V to improve the management of the IT acquisition/development program.	*Not met.* USCG officials stated that they did not use risk-based criteria to determine that IV&V should be performed on C4ISR because they thought DHS mandated the use of IV&V. The USCG identified documents containing its IV&V approach, policies, and standards, but these documents do not include a process for using IV&V results to improve program management.
IV&V effort independence. The degree of technical, managerial, and financial independence required of the personnel or agents performing IV&V is defined, including (1) technical, managerial, and financial independence requirements for the IV&V agent; and (2) a mechanism for reporting the results of IV&V to program oversight officials, as well as program management.	*Partially met.* C4ISR's IV&V activities are performed by a mix of internal and external organizations that are all third parties to the development team, and thus are, to a certain degree, independent. Nevertheless, C4ISR did not demonstrate that it has specific controls in place to ensure the full technical, managerial, or financial independence of its IV&V agents. In addition, C4ISR's statement of work for security and testing IV&V efforts states that monthly IV&V status reports are to be provided to a program management official. However, it does not call for reporting IV&V results to program oversight officials. In addition, USCG did not provide documentation that describes a mechanism for reporting results of other IV&V activities, such as cost estimation.
IV&V program scope. The scope of IV&V activities is defined, including (1) a definition of the program activities subject to IV&V; and (2) validation and verification compliance criteria for each program activity subject to IV&V.	*Partially met.* C4ISR's IV&V statement of work defines the scope of IV&V for several activities, such as security risk assessment and assessing the adequacy of test and evaluation. However, not all IV&V activities identified by USCG were defined and documented. Further, USCG did not document compliance criteria for its IV&V activities.
IV&V program resources. The resources needed for IV&V are specified, including (1) the facilities, personnel, tools, and techniques and methods.	*Partially met.* USCG defined IV&V resource needs for security and test-related activities, including information on subject matter expertise required. However, USCG did not provide descriptions of IV&V resource needs for other activities, such as performance verification.
IV&V management and oversight. The management and oversight to be performed are specified, including (1) the process for responding to issues raised by the IV&V effort; (2) the roles and responsibilities of all parties involved in the program; and (3) how the effectiveness of the IV&V effort will be evaluated.	*Partially met.* USCG did not provide a documented process for responding to issues raised by IV&V efforts. C4ISR's IV&V statement of work for security and test-related program activities defines roles and responsibilities. For example, it defines the IV&V unit's responsibility for performing six major services and lists specific deliverables. It also identifies USCG technical and contractual responsibilities. Additional responsibilities for USCG officials are described in the *Major Systems Acquisition Manual*. However, while the manual describes responsibilities for several government officials, it does not identify responsibilities related to IV&V. Furthermore, the C4ISR IV&V statement of work identified specific tasks and deliverables related to testing and security activities. For example, the IV&V team is to assess test and evaluation plans and procedures and provide recommendations. However, USCG did not identify how it evaluates the effectiveness of the IV&V effort, including its recommendations.

Source: GAO analysis of DHS data.

U.S. Citizenship and Immigration Services (USCIS)—Transformation Program (Transformation)

Transformation is a 5-year effort to modernize business processes and information technology throughout USCIS. The goal of the program is to move USCIS from a paper-based filing system to a centralized and electronic filing system. It is a level 1 acquisition, and its current life cycle cost estimate is $1.7 billion; however, the LCCE is under review. The program has budgeted approximately $62 million for IV&V services. There are five segments of the program; four segments are in the planning phase, and one is in the requirements definition phase.

USCIS reports that the IV&V agent is currently reviewing or plans to review the following activities:

- independent cost estimation or cost estimate validation;
- program progress or performance verification or evaluation;
- requirements validation or verification;
- concept or design validation, verification, or alternatives analysis;
- risk evaluation;
- security vulnerability or security risk assessments;
- configuration management verification;
- component verification testing and evaluation;
- system or integration verification testing and evaluation; and
- operational readiness testing and evaluation.

Table 15 describes the extent to which the program has implemented the key elements of effective IV&V.

Table 15: Transformation's Implementation of the Key Elements of Effective IV&V

Key element	Summary of implementation
Decision criteria. A risk-based, decision-making process is defined to determine whether or the extent to which programs should be subject to IV&V, to include (1) establishing risk-based criteria for determining which programs should be subject to IV&V; and (2) establishing a process for using IV&V to improve the management of the IT acquisition/development program.	*Not met.* USCIS officials stated that their policy, as well as DHS policy, requires that all level 1, 2, and 3 projects perform IV&V. However USCIS did not provide a policy containing that requirement. Moreover, as discussed previously in this report, DHS's guidance does not require the use of IV&V, nor does it establish or require the use of risk-based decision-making process for determining whether or to what extent to conduct IV&V. As such, USCIS did not provide evidence that USCIS's decision for Transformation was risk-based. In addition, documentation provided by Transformation did not indicate that it has a documented process for using IV&V to improve the management of the program.
IV&V effort independence. The degree of technical, managerial, and financial independence required of the personnel or agents performing IV&V is defined, including (1) technical, managerial, and financial independence requirements for the IV&V agent; and (2) a mechanism for reporting the results of IV&V to program oversight officials, as well as program management.	*Partially met.* Transformation provides for technical independence by documenting in the IV&V statement of work that IV&V contractors are prohibited from soliciting, proposing, or being awarded efforts related to USCIS IT programs or services. However, Transformation has not documented requirements for the managerial and financial independence of its IV&V agents. Moreover, the IV&V statement of work requires the contractor provide reports that document their findings and recommendations. While officials stated that they had a mechanism to ensure IV&V reports are provided to both program oversight officials and program management, they did not provide documentation to support this.
IV&V program scope. The scope of IV&V activities is defined, including (1) a definition of the program activities subject to IV&V; and (2) validation and verification compliance criteria for each program activity subject to IV&V.	*Partially met.* The statement of work for Transformation identifies and defines IV&V activities and their associated tasks. However, the statement of work establishes compliance criteria for some, but not all, of the activities subject to IV&V. For example, the IV&V statement of work requires the agent to evaluate certain test plans for compliance with specific federal statutory and regulatory guidance. On the other hand, the same task order also requires the agent to determine if certain error rates are "manageable", without defining what that term means. In its technical comments and a subsequent interview, USCIS and Transformation officials stated that they have established compliance criteria for program activities that are subject to IV&V. They also provided several other documents, including detailed checklists related to assessing the quality of certain user requirements documents. However, neither these documents, nor the IV&V statement of work, indicate that the IV&V agent is to use these checklists as evaluation criteria. Further, written comments in these documents, made by USCIS's Chief of the Process Control Branch, indicate that these checklists are, in fact, still being developed.
IV&V program resources. The resources needed for IV&V are specified, including (1) the facilities, personnel, tools, and techniques and methods.	*Met.* The IV&V statement of work for Transformation lists the resources required to perform IV&V, including personnel, facilities, training, and tools. For example, it outlines the necessary training, certification, and tools needed for IV&V activities related to IT security auditing.

Key element	Summary of implementation
IV&V management and oversight. The management and oversight to be performed are specified, including (1) the process for responding to issues raised by the IV&V effort; (2) the roles and responsibilities of all parties involved in the program; and (3) how the effectiveness of the IV&V effort will be evaluated.	*Partially met.* Transformation officials did not provide a documented process for responding to issues that are raised by the IV&V agents. In addition, the contractor's role and responsibilities are documented throughout the IV&V statement of work for Transformation, but no documentation was provided defining the IV&V roles and responsibilities of USCIS officials. Finally, officials did not provide a process for evaluating the effectiveness of its IV&V program. In its technical comments, USCIS and Transformation officials stated that government roles and responsibilities for IV&V are defined in DHS and USCIS guidance which they previously provided. While some of the reviews in USCIS's documents are specified as being independent, they are part of the system lifecycle, rather than a separate review of products and outcomes. As we described previously in this report, IV&V is work above and beyond the normal quality assurance and performance review activities performed during system development and/or acquisition.

Source: GAO analysis of DHS data.

Appendix V: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

July 19, 2011

David A. Powner
Director, Information Technology Management Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Draft Report GAO 11-581, "INFORMATION TECHNOLOGY: DHS Needs to Improve Its Independent Acquisition Reviews"

Dear Mr. Powner:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO's) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's positive acknowledgement of actions DHS has taken in establishing key institutional acquisition and Information Technology (IT) investment management-related controls and implementing them on large-scale programs. DHS is committed to continuing efforts to instill more discipline and rigor in its acquisition and IT processes.

The draft report contained three recommendations, which DHS concurs. Specifically, to help guide consistent and effective execution of Independent Verification and Validation (IV&V), GAO recommended that the Secretary of Homeland Security direct the Department's Chief Information Officer and Chief Procurement Officer to:

Recommendation 1: Revise DHS acquisition policy such that it establishes:

- risk-based criteria for (1) determining which major and other high-risk IT acquisition programs should conduct IV&V, and (2) selecting appropriate activities for independent review of these programs;
- requirements for technical, financial, and managerial independence of agents;
- standards and guidance for defining and documenting plans and products;
- controls for planning, managing, and overseeing efforts;
- mechanisms to ensure that plans and significant findings inform DHS acquisition program reviews and decisions, including those of the ARB; and
- monitor and ensure implementation of this policy on applicable new IT acquisition programs.

Response: Concur. DHS is prepared to leverage its current Directive Number 102-01, Revision Number: 01, Acquisition Management Directive (MD) policy to evoke an interim IV&V standard to provide a common-language framework describing best practices, templates, tools, and processes to engage when implementing IV&V into the work environment. This policy will also include IV&V approaches when monitoring and controlling IV&V in a post-implemented environment such as operations and maintenance and life-cycle management.

Directive 102-01 provides the overall policy and structure for acquisition management within DHS which describes the Department's Acquisition Life Cycle Framework (ALF), Acquisition Review Process (ARP), and Acquisition Review Board (ARB). Within Directive 102-01, Appendix B is the System Engineering Lifecycle (SELC) Guide (ver. 2.0). The SELC provides a framework for development using proven systems engineering principles, processes, documentation, and reviews tailored to satisfy unique circumstances of the program/project early in the life of the program. SELC reviews are used to inform Component/departmental oversight structure (e.g., ADE reviews) on progress toward successful capability development.

Current SELC reviews include:

- Project Planning Review
- System Definition Review
- Preliminary Design Review
- Critical Design Review
- Test Readiness Review
- Production Readiness Review
- Operational Readiness Review

DHS will review Appendix B (SELC) in consideration of modifying the framework to adapt to IV&V industry standards and best practices, which includes "Systems Requirements Definition" and "Integration Testing." IV&V guidance will ensure adequate controls and oversight are implemented for requirements management[1] to (1) effectively manage the Department's acquisition, (2) effectively identify risks, and (3) ensure proper controls are established for the Department to manage its acquisition process efficiently. Integration serves to verify and validate that the design transformations are correct, accurate, and satisfy operational requirements for end-user performance. DHS continues its commitment to improve processes for operational efficiencies and integration strategies that will migrate operations closer in alignment with business strategies.

The Directive also provides additional management procedures and responsibilities that augment the existing policies, regulations, and statutes that govern the procurement and contracting aspects of acquisition. In general, the policy describes the complexity of relations within DHS and its Stakeholder environment. The modified SELC, which will include IV&V guidance, will show evidence of independence in key areas of technical, managerial, and financial independence as defined within GAO's report.

[1] DHS ARB allows DHS to manage and identify risks in the acquisition process. The most important phase of the acquisition process is the requirements phase; therefore, it is very important that in the acquisition life cycle, management focuses considerable attention on working with Components using "risk-based" approaches to ensure requirements are understood and expected outputs are equally understood in order to produce an effective acquisition outcome.

2

Where DHS high-priority investments are obligatory, each investment is required to certify that the investment is under an IV&V contract. In accordance with MD 102-01, supporting documentation must confirm this compliance. In addition to major IT investments having an IV&V contract within scope, certification criteria must confirm:

- Contractor IV&V approach meets Institute of Electrical and Electronics Engineers (IEEE) 1012 standards.
- Contractor approach ensures artifacts are complete, of sufficient quality, and satisfy user requirements.
- Contractor IV&V technical approach includes all necessary IV&V activities.
- Contractor IV&V technical approach identifies a strategy or method for determining which activities are conducted, how those activities will be performed, and when those activities will be executed.

The DHS Office of the Chief Information Officer (OCIO) will consider revising the DHS acquisition policy such that it establishes review of vendor contracts ensuring that certification criteria is met, as well as, include internal controls for oversight of IV&V implementation (e.g.,ARB) . In addition, DHS OCIO will require the development of an IV&V plan at the initial project's life cycle, and an IV&V Assessment Project Review at the conclusion and delivery of the program validating that all artifacts, processes, and systems are developed in accordance with customer requirements, in addition to being well-engineered. DHS Components will be expected to use the IV&V Plan to tailor activities within the Component depending on program size, complexity, risk, and other program management factors.

The combination of 22 federal agencies under one DHS leadership, each having its own legacy systems and processes, requires normalization through standardization. IV&V guidance to be modified within Directive 102-01 will normalize and set standards DHS-wide.

Recommendation 2: Re-evaluate the approach to IV&V for ongoing programs (including the eight programs featured in this report) and ensure that appropriate action is taken to bring each of them into alignment with the elements of leading practice.

Response: Concur. DHS has routinely practiced monitor and control of its major IT investments. In 2005, it created MD 1400 – Investment Review Process with the primary purpose of ensuring that spending on investments directly supports and furthers DHS's mission and provides optimal benefits and capabilities to stakeholders and customers. In 2007, DHS issued MD 0007.1 Information Technology Integration and Management establishing the DHS vision and the authorities and responsibilities of the Department's OCIOs as "shared leadership" in alignment with the integration of its acquisition governance. A year later, DHS Acquisition Program Management Division (APMD) published an interim DHS Directive 102-01 and Guidebook D-102-01-001 v1.9, (November 2008). This Guidebook overhauled the DHS acquisition management system and superseded all versions of DHS MD 1400, Investment Review Process. Directive 102-01 was made permanent in January 2010. This update created provisions for an improved ALF, ARP, and ARB.

3

Together, these three bodies enable oversight of DHS's major IT investments for developmental pre- and-post programs.[2]

DHS Directive Number 102-01, Revision Number: 01, Acquisition MD, Issue Date: 01/20/2010, recognizes IV&V as a leading practice and recommends (though does not require) its use within DHS with the exceptions of when IV&V activities are mandated by Congress and when required by the ARB. The Guidebook also has limited information and guidance on the formation and delivery of IV&V practices.

However, the DHS Headquarters (HQ) OCIO Draft IV&V Policy Implementation Plan is being developed to provide a common language framework describing best practices, templates, tools, and processes to engage when implementing IV&V into the work environment. This framework will also include IV&V approaches when monitoring and controlling IV&V in a post-implementation environment, such as operations and maintenance and life-cycle management. The IV&V document will either be inserted into the SELC process or used as a "stand-alone" document for quality assurance measures of all DHS programs (including the eight programs featured in this report) to bring all into the IV&V practice for major IT investments.

HQ OCIO is responsible for overseeing the governance process of interdependencies between DHS capital planning, investments, programs, and projects. Although OCIO interacts with DHS Components to provide best-practice guidance, templates, and tools concerning industry-leading techniques, DHS Components retain the authority to set internal acquisition processes and procedures, as long as the processes and procedures are consistent with the intent of the Acquisition MD.

DHS IV&V will establish a methodology for documented evidence that a DHS process, artifact, or system under IV&V performs its intended functions correctly. The result is knowledge that the process, artifact, or system will do what it has been designed to do and will continue to perform correctly in the future to measure its quality and reliability and render evidence that the process, artifact, or system functionality is traceable to system requirements.

Finally, DHS IV&V, at the Component level, will reinforce the role of the Program Manager in establishing the planning and execution of the IV&V process. This includes assigning the program management team to daily tasks, under an independent contract and/or as part of the program management team; coordinating and interpreting the team's performance and quality; reporting discrepancies promptly to internal/external groups; identifying early problem trends; focusing team activities; providing a technical evaluation of the product's cost, performance, and quality at each major program review; and assessing the full effect of proposed product changes. DHS IV&V, at the HQ level, will engage an independent team of subject matter experts to administer oversight of the IV&V implementation process, validating that appropriate resources, certifications, tools and facilities were allocated to meet

[2] Since June 2010, APMD has added program analysts to support the Components; which have enabled APMD to dedicate additional hours in the direct assistance to each program and to ensure that appropriate corrective actions are accomplished. With improved coverage for Components and programs, APMD is a much more familiar participant in program reviews and update activities. In addition, the added resources and personnel to APMD have allowed the Deputy Secretary and the Under Secretary for Management greater governance oversight of major Department-wide acquisitions. Additional personnel have allowed APMD to push more Level 1 and 2 programs through the ARB process.

the expectations of the requirements. This Integrated Project Team will report managerial, financial and technical results, as necessary.

Recommendation 3: Collect and analyze data on IV&V efforts for major IT acquisition programs to facilitate the development of lessons-learned and evaluation of the effectiveness of DHS' investments, and establish a process that uses the results to inform the department's IT investment decisions.

Response: Concur. DHS recognizes challenges in IV&V data collection reserved for future evaluation and consistency. To demonstrate improvement in this area, DHS will focus the "A-B-Cs" of IV&V data collection for its major IT investments in the following areas:

- ARP (using a program's size, complexity, and risk [cost, schedule, performance])
- Baseline/Benchmark (test data, reports, requirements, deliverables, industry standards)
- Contractor IV&V Certification (independent test, validation, verification, evaluation solutions)

IV&V Tool	Entry Criteria
ARP	DHS initially reviews its portfolios (E300s and E53s) on an annual basis. This process allows Component CIOs to present IT investments before the DHS CIO and APMD for funding approval, evaluation consideration, and continuance.
Baseline/Benchmark	Acquisition Program Baseline defines the critical cost, schedule, and performance parameters for the investment and is the baseline against which programs report their progress. Industry standard best practices create industry standard benchmarks.
Contractor (IV&V) Certification	Contractor IV&V approach meets IEEE 1012 standards; Contractor approach ensures artifacts are complete, of sufficient quality, and satisfy users requirements; Contractor IV&V technical approach includes all necessary IV&V activities; Contractor IV&V technical approach identifies a strategy or method for determining which activities are conducted, how those activities will be performed, and when those activities will be executed.

It is important for DHS to achieve success in the implementation and guidance of IV&V across its programs and projects. As DHS continues evolving the practice of IV&V within development life cycles and uses the results of each repeatable process to analyze and improve cycle time, the data collected and documented for further review will benefit DHS by:

- focusing understanding on stakeholder requirements resulting in meeting or exceeding customer expectations
- gauging metrics to measure performance to ensure quality and effectiveness are met
- maximizing efficiencies through the use of resources (people, tools, facilities), exemplifying identified required skills and knowledge
- providing opportunity for staff to achieve a common understanding of process modeling, theories, and best practices

DHS will store this data collection in a repository for the purpose of showing Lessons Learned practices that support the organization's goals to promote recurrence of successful program outcomes and preclude the recurrence of unsuccessful outcomes. This data

5

collection is to be tailored to fit the complexity, scope, size, cost, and risk of the major IT investment.

Again, thank you for the opportunity to review and comment on this draft report. Technical comments were submitted under separate cover. We look forward to working with you on future Homeland Security related issues.

Sincerely,

Jim H. Crumpacker
Director
Departmental GAO/OIG Liaison Office

6

Appendix VI: GAO Contact and Staff Acknowledgments

GAO Contact

David A. Powner at (202) 512-9286 or pownerd@gao.gov

Staff Acknowledgments

In addition to the individual named above, the following staff also made key contributions to this report: Paula Moore (Assistant Director), Neil Doherty, Lynn Espedido, Rebecca Eyler, Nancy Glover, Daniel Gordon, Jim Houtz, Justin Palk, and Shawn Ward.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Please Print on Recycled Paper